MIGRACION DE UN SERVIDOR WINDOWS A LINUX

David Martínez Sanz

Director de Proyecto: Lenin Lemus Zúñiga

Codirector de proyecto: Agustín Espinosa Minguet

Departamento de Informática de Sistemas y Computadores

DISCA

Escola Tècnica Superior d'Informàtica Aplicada

UNIVERSIDAD POLITECNICA DE VALENCIA

Realizado con LaTeX

Índice

1. Introducción.

> *From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds) Newsgroups: comp.os.minix Subject: What would you like to see most in minix? Summary: small poll for my new operating system Message-ID: <1991Aug25.205708.9541@klaava.Helsinki.FI> Date: 25 Aug 91 20:57:08 GMT Organization: University of Helsinki Hello everybody out there using minix - I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) (among other things). I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-) Linus (torvalds@kruuna.helsinki.fi) PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT protable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.*

1.1. Motivación.

Entre los principales motivos que mueven a muchas empresas y organismos públicos a migrar a sistemas abiertos que todavía utilizan sistemas basados en Windows NT es la falta de continuidad de soporte técnico que Microsoft dejó de ofrecer hace bastante tiempo.

Otros motivos imputables, es el cambio de la estrategia de las TI en la que se apoya los sistemas de información: diversificación de software, mejora de la interoperabilidad de los sistemas, flexibilidad, robustez, estabilidad, rendimiento, etc...

Linux es un sistema operativo basado en UNIX y compatible con POSIX que se distribuye bajo licencia GNU, este tipo de licencia permite la libre distribución y modificación del código fuente del sistema operativo, además Linux forma parte del software de código abierto(OSS) el cual posee diversos beneficios entre los que se encuentran la libre competencia entre proveedores no limitándose a un único proveedor.

Linux implementa completamente la pila de TCP/IP , lo que permite que soporte gran cantidad de clientes y servicios, incluyendo la programación

del interfaz socket. Todos los programas que utilicen TCP/IP pueden ser portados fácilmente a Linux.

En referencia al hardware, muchas distribuciones pueden funcionar en equipos antiguos o no actualizados, lo que permite la reutilización del hardware que no soportaría los requerimientos de sistemas operativos Windows. Por otra parte la estructura modular del kernel de Linux en forma de módulos facilita la actualización y parcheado del sistema sin necesidad de reiniciar el equipo y puede realizarse mientras otras aplicaciones continúan en ejecución(algo crítico para los sistemas dedicados).

2. Diferentes alternativas de migración.

2.1. Definiciones.

2.1.1. Software Open Source.

Software Open Source(OSS): OSS permite que cada usuario pueda leer y modificar libremente el código fuente, lo que permite que dichos usuarios puedan aprender y/o adaptar el código fuente a sus requerimientos personales y necesidades. El código es libremente accesible y no es necesario abonar ninguna licencia. La única condición es que el software modificado debe ser copiado y distribuido libremente.

2.1.2. Software propietario.

Software Propietario: el software propietario pertenece a una persona individual o a una organización, normalmente el desarrollador del software(copyright). El uso del software se encuentra sujeto a los términos de la licencia bajo la cual se encuentra el software propietario. Entre estos términos se encuentran la prohibición de duplicación y modificación del software.

2.1.3. Software Linux comercial.

Software Linux Comercial: incluye al conjunto de productos de software propietario que se ejecutan bajo el sistema operativo Linux.

2.2. Infraestructura de la migración.

2.2.1. Microsoft Windows como situación inicial.

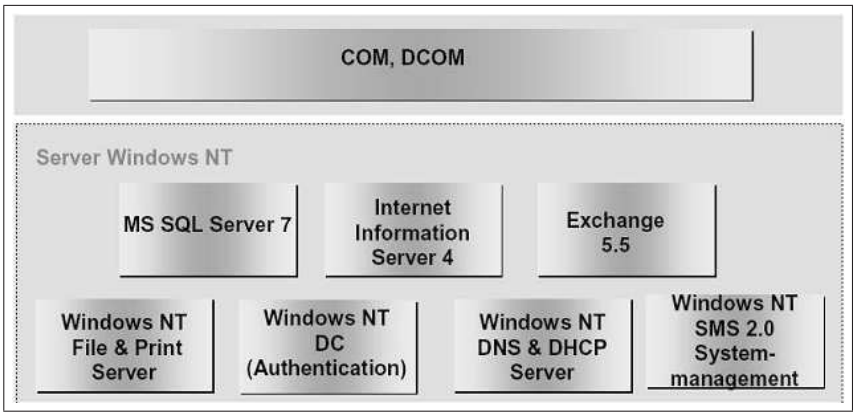

Figura 1: Escenario de sistemas Windows

La ilustración de la figura 1 muestra el escenario de sistemas Windows que puede encontrarse generalmente, esta imagen muestra un resumen de los servicios y módulos software que pueden formar parte de una situación inicial del análisis de migración.

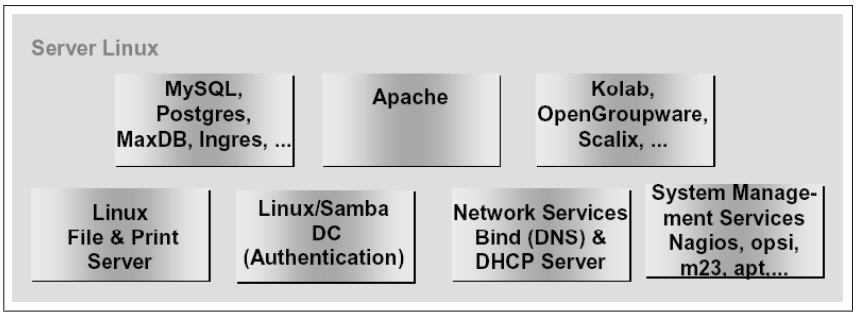

Figura 2: Escenario de sistemas Linux

La ilustración de la figura 2 representa una típica solución viable basada en Linux, se muestra el conjunto de software Open Source utilizado para sustituir a los servicios de red empleados por Windows. Principalmente nos centraremos en el supuesto de un servidor con Windows 2000 Server que realiza las funciones de servidor de archivos, autenticación y gestión de usuarios y DNS(escenario típico de Directorio Activo).

2.2.2. Distribuciones Linux.

Existen gran cantidad de distribuciones Linux disponibles para implementar sistemas servidores. A parte del sistema operativo "puro" estas distribuciones incluyen gran cantidad de paquetes software que ofrecen una amplia funcionalidad y versatilidad. Generalmente éstas distribuciones son desarrolladas para facilitar la instalación del kernel del sistema operativo y todos los programas asociados. Las compañías de éstas distribuciones han desarrollado e incluido herramientas administrativas para configurar el software que acompaña al sistema operativo y su kernel. Cuando alguien adquiere una distribución no compra Linux "en sí mismo" sino un compendio formado por el sistema operativo, programas de utilidades e instalación y la documentación técnica creada por el distribuidor.

Las diferentes distribuciones se encuentran disponibles como paquetes completos(CD, documentación) comerciales y en algunos casos como copias libres que pueden ser descargadas desde Internet, los paquetes en formato comercial generalmente suelen incluir servicios de soporte proporcionados por el distribuidor que no se encuentran en versiones descargadas de Internet. La compatibilidad entre versiones de Linux y la estandarización de las distintas distribuciones son cuestiones a tener en consideración, para evitar diferencias inaceptables entre distribuciones individuales fue creada la estructura de directorios para Linux(*Filesystem Hierarchy-Standard*) que está integrada en la *Linux Standard Base* cuya principal función es conseguir la máxima compatibilidad entre todas las distribuciones.

Debian GNU Linux

El proyecto Debian es el resultado de un esfuerzo voluntario para crear un sistema operativo libre de alta calidad, compatible con Unix y acompañado de una gran cantidad de aplicaciones. En analogía con el desarrollo del kernel de Linux, los miembros que forman el proyecto Debian desde todos los lugares del mundo son profesionales envueltos en el desarrollo de ésta distribución, por ese motivo Debian es denominada la distribución “de profesionales para profesionales“. Las principales ventajas de ésta distribución son:

- Completo: Debian incluye más de 15180 paquetes de software en este momento. Los usuarios pueden seleccionar qué paquetes instalar; Debian provee una herramienta para ese fin. Encontrará una lista con las descripciones de los paquetes actualmente disponibles con Debian en cualquiera de los sitios réplica de Debian.

👍 Libre para utilizar y redistribuir: No se requiere ninguna clase de cuota para ser socio de ningún consorcio, ni pago solicitado para participar en su distribución y desarrollo. Todos los paquetes que formalmente son parte de Debian GNU/Linux son libres para ser redistribuidos, normalmente bajo los términos especificados por la Licencia Pública General de GNU.
Los archivos FTP de Debian también tienen aproximadamente 220 paquetes de software (en los directorios non-free y contrib de los archivos FTP), los cuales se distribuyen bajo términos específicos que se incluyen con cada paquete.
👍 Dinámico: Con alrededor de 1570 voluntarios constantemente contribuyendo con código nuevo y mejorado, Debian evoluciona rápidamente. Se planea realizar nuevas entregas cada varios meses, y los archivos FTP se actualizan diariamente.

👎 En el lado de desventajas hay que decir que Debian tiene un mayor componente técnico que otras distribuciones. También, dada la naturaleza voluntaria de los desarrolladores, es posible que ciertos paquetes no estén tan actualizados como debieran, quizás porque sus desarrolladores han dejado de actualizarlos y nadie se ha hecho cargo. Sin embargo esto es algo que todos los desarrolladores tratan de evitar y, aunque cada desarrollador mantiene sus paquetes, no es raro que otro desarrollador (incluso un usuario) envíe una nueva versión del paquete para arreglar un problema o actualizarlo.

Red Hat Linux

La distribución comercial Red Hat ofrece a sus clientes diferentes alternativas para diferentes aplicaciones:

Producto	**Aplicación**
Red Hat Enterprise Linux AS	Grandes bases de datos y entornos críticos(24x7).
Red Hat Enterprise Linux ES	Servidores de ficheros y web de software.
Red Hat Enterprise Linux WS	Aplicaciones de alto rendimiento para escritorio
Red Hat Desktop	Entorno multiusuario, sector SOHO

Cuadro 1: Productos Red Hat

La principal diferencia entre los productos ofertados por Red Hat son sus diferente aplicaciones y el alcance de soporte ofertado, en los acuerdos de licencia disponibles y el precio de compra. El formato de paquetes propuesto por Red Hat (rpm, Red Hat Package Management) ofrece un manejo amigable y uniforme para la administración de software.

Suse Linux

A finales del año 2003 la norteamericana Novell adquirió al distribuidor alemán de Linux llamado Suse por lo cual se convirtió en si misma distribuidora de Linux. En la siguiente tabla se muestran los distintos productos de Suse Linux:

Producto	**Aplicación**
Suse Linux Enterprise Server	Entornos críticos(24x7) y grandes entornos de prod.
Suse Linux Professional	Aplicaciones para escritorio, incluye gran cantidad de software.

Cuadro 2: Productos Suse

La distribución Suse(al igual que RedHat) está basada en el sistema de paquetes de software RPM, pero el método de instalación y administración es distinto, está integrado en la aplicación YaST. Al igual que otras distribuciones las principales diferencias entre las opciones comerciales de Suse que aparecen en la tabla anterior están basadas en el soporte ofrecido: soporte 24x7, servicios personalizados y certificaciones de distintas aplicaciones.

3. Servicios disponibles en Windows y Linux en la actualidad.

3.1. Servicios de red TCP/IP básicos.

El direccionamiento IP constituye la base de casi todas las redes actuales, incluida Internet. Los servicios de DNS, DHCP *(Dynamic Host*

Control Protocol) y de tiempo *(NTP)* son normalmente los primeros que se ejecutan en una red, ya que constituyen los requisitos esenciales para poder poder utilizar todos los demás servicios de red.
DHCP es el protocolo de red que asigna dinámicamente las direcciones IP y los parámetros de red necesarios para configurar debidamente los hosts. Si bien la mayor parte de los servidores utilizan direcciones IP estáticas, las estaciones de trabajo(sobre todo si el número es amplio)reciben normalmente direcciones IP dinámicas, así como otra información de red que les permiten comunicarse con otros con hosts de la red.
La mayor parte de los portátiles y equipos de escritorio no utilizan direcciones IP estáticas, sino que reciben la dirección IP de un servidor DHCP. Tras un reinicio o al caducar una concesión, la estación de trabajo se pondrá en contacto con el servidor DHCP para renovar la concesión y obtener una nueva dirección IP.
Los servicios de resolución de nombres(DNS) son otra parte importante de la infraestructura de una red de ordenadores. La capacidad de transformar nombres de hosts de palabras sencillas en direcciones IP constituye una función esencial de las redes de todo tipo y tamaño, desde las LAN de pequeñas empresas a Internet, la red mundial. DNS ofrece esta funcionalidad a Windows y Linux.

El último de los servicios de red básicos permite sincronizar los relojes en todos los ordenadores de la red. Aunque algunas partes de una red de ordenadores pueden funcionar perfectamente sin que los relojes estén sincronizados, para otros servicios es imprescindible.

3.2. Servicios de directorio.

Los servicios de directorio son un componente esencial en la gestión y la catalogación de objetos, como las cuentas de usuario y las configuraciones de los perfiles, grupos, ordenadores, impresoras, e-mail, y otros objetos de la infraestructura de red. Un servicio de directorio típicamente consiste en una base de datos en la cual se almacenan los componentes de red mencionados anteriormente, el protocolo comúnmente utilizado actualmente para ello es LDAP*(Lightweight Directory Access Protocol)*. Una característica principal de este protocolo es la disposición de una estructura jerárquica de la información almacenada, llamada árbol de información de directorio o DIT, la estructura del DIT comienza con el DN base(sufijo o *distinguised name*) y está se parado lógicamente por objetos de unidad organizativa(ou). Los DIT se organizan normalmente según el tipo de objetos contenidos en cada árbol. En algunas circunstancias, la organi-

zación geográfica o de unidades de negocio puede afectar al diseño de los DIT.

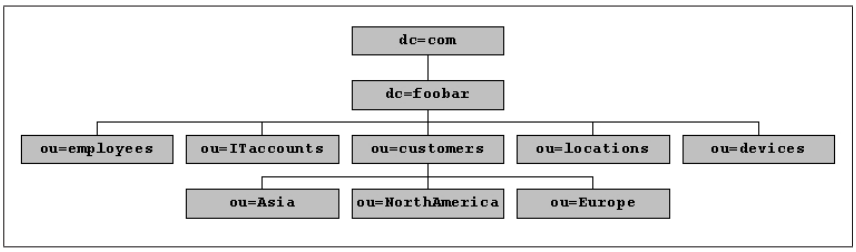

Figura 3: Arbol de información de directorio

Cada uno de los objetos del árbol de directorio se identifica de manera unívoca con un nombre distinguido, o DN, que se compone del atributo que identifica unívocamente al objeto(normalmente en nombre común, o CN, o ID del usuario, uid) seguido por la ruta en la que se ubica el objeto en el DIT. Por ejemplo el DN de un usuario que perteneciera a la ou de Asia sería: *cn=user,ou=Asia,ou=Costumers,dc=foobar,dc=com*

Un directorio es un almacén jerárquico de objetos y sus atributos. Cada objeto es una instancia de una o más clases de objetos. Las clases de objetos definen el conjunto de atributos que pueden o deben contener esos tipos de objetos, que pueden ser texto, datos binarios u otro tipo de información.
El conjunto de clases de objetos que admite un servidor de directorio se llama esquema del directorio. Los archivos de esquema contienen definiciones de sintaxis, atributos y clases de objetos. Cada una de esas entidades se asocia con un identificador de objeto(OID) que se representan mediante una notación decimal separada por puntos e identifican de forma unívoca las definiciones de sintaxis, atributos y objetos, un ejemplo es la definición de objeto *persona* extraída del esquema *core.schema*:

objectclass (2.5.6.6 NAME 'person' SUP top STRUCTURAL
MUST (sn $ cn)
MAY (userPassword $ telephoneNumber $ seeAlso $ description))

En esta definición de clase de objeto se enumeran los atributos que debe(MUST) contener un objeto persona(*nombre completo y apellidos*) y los atributos que pueden(MAY) aparecer opcionalmente(*userPassword, telephoneNumber, seeAlso y Description*). La descripción de estos atributos aparecen en otra parte de archivo:

attributetype (2.5.4.3 NAME ('cn' 'commonName') SUP name)
attributetype (2.5.4.4 NAME ('sn' 'surname') SUP name)
attributetype (2.5.4.35 NAME 'userPassword'
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40128)

Para poder realizar operaciones tales como consultas LDAP, los clientes deben conectarse en primer lugar al servidor de directorio. En la jerga de LDAP esta operación es denominada *bind*, y existen varios tipos:

- Bind anónimo.
- Bind sencillo.
- Bind sencillo con TLS.
- Bind sencillo con SASL.

En un bind anónimo, el cliente LDAP proporciona un DN y una contraseña de binding vacíos. En un bind con autenticación el cliente LDAP proporciona el DN del objeto de directorio con el que hay que realizar el bind y las correspondientes credenciales, como una contraseña, que en este caso viaje en texto claro por lo que es más recomendable emplear algún tipo de encriptación como TLS o SASL.

Los servicios de directorio de Microsoft

Windows NT y Windows 2000 Server utilizan tres servidores de directorio: el Administrador de cuentas de seguridad(SAM) de NT, los servicios de directorio de Exchange 5.5 y Windows 2000 Active Directory, sólo se va a comentar éste último que es el servicio realmente implicado en el proceso de migración.
Active Directory implementa un interfaz LDAP, aunque el método más ampliamente utilizado para acceder a los objetos de Active Directory es la interfaz de servicios de Active Directory(ADSI). AD(Active Directory) está estrechamente integrado con las implementaciones de DNS y DHCP y requiere que los servicios DNS para funcionar correctamente. AD permite almacenar una gran cantidad de objetos entre los que se incluyen nombres de usuario, nombres completos, descripciones, hashes de contraseñas, directorios principales, rutas de perfiles, y un largo etc...

OpenLDAP

OpenLDAP es la principal solución de directorio de código abierto. Contiene una suite completa con todos los componentes de cliente y servidor necesarios para implementar y utilizar los servicios de directorio. OpenLDAP funcio-

na en todas las versiones de Linux y cuenta con una sólida compatibilidad de replicación para servicios de directorio distribuidos. Está implementado mediante dos servicios(demonios):

- Slapd: es el proceso del servidor que escucha en los puertos de red y responde a las conexiones LDAP de los clientes.
- Slurpd: es el proceso ofrece funciones de replicación, por lo que permite disponer de servicios de directorio distribuido, puede trabajar con modelos de replicación maestro-esclavo(maestro único) o maestro-maestro(múltiples maestros). En la replicación maestro-esclavo se mantiene una única copia de lectura-escritura(el maestro) del directorio, que se replica a una o más copias de sólo lectura(los esclavos). Slurpd lleva a cabo réplicas de tipo *push*, es decir, el maestro inicia las conexiones con los otros servidores y les envía(push) actualizaciones.

En la replicación de múltiples maestros, varios servidores de directorio pueden escribir en el directorio. Cuando se realiza un cambio, el servidor de directorio que procesa la operación de escritura envía una actualización a los demás servidores de directorio.

3.3. Servicios de autenticación.

La autenticación es uno de los servicios más importantes y de uso más extendido. La capacidad de controlar el acceso a los recursos de la red depende esencialmente de la capacidad de determinar quién es el usuario, la autenticación de este usuario pasa por la validación de credenciales de uno o más elementos: algo que se conoce (nombre de usuario, contraseña), algo que se posee (objeto) o algo que se es (biometría). Los requisitos de seguridad, escalabilidad, fiabilidad y funcionalidad de cualquier empresa implican que será necesario usar un sistema de seguridad que interactúe con un servicio de directorio y de archivos, las credenciales de autenticación se almacenan en el directorio, no en el servicio de autenticación. Con un directorio que actúe como repositorio centralizado de esta información, es posible gestionar sistemas de autenticación flexibles que permitan centralizar el control de servicios de autenticación.

Autenticación en Windows

Microsoft presentó un mecanismo de autenticación basado en *Kerberos*, Kerberos es un protocolo de autenticación de red. Esta diseñado para suministrar una autenticación poderosa para aplicaciones cliente/servidor usando criptografía de clave pública o asimétrica. La implementación de Kerberos de

Microsoft interactúa con muchos servidores que ejecutan servicios de código abierto o diferentes al sistema Kerberos de Microsoft.
El proceso de inicio de sesión en Windows 2000/XP por defecto, intenta realizar una autenticación mediante Kerberos, aunque también son compatibles con la autenticación NTLM. Kerberos es más flexible, eficiente y seguro que NTLM, protocolo de autenticación anteriormente utilizado en Windows NT y 98, está compuesto por 3 sub-protocolos:

- AS Exchange(Servicio de autenticación de intercambio): proporciona un ticket de inicio de sesión al cliente(*TGT, Ticket Granting Ticket*).
- TGS Exchange(*Ticket Granting Service*): proporciona una llave de servicio de sesión.
- CS Exchange(*Client/Server Exchange*): envía el ticket de acceso al servicio desde el cliente al servidor.

Autenticación en Linux

Históricamente, UNIX dispone de métodos de autenticación desde hace más de cuarenta años. Desde el venerable /etc/passwd a los PAM de hoy en día, se han utilizado multitud de métodos de autenticación en los inicios de sesión de las estaciones de trabajos *NIX.
La información de usuarios se almacena en /etc/passwd y la de las contraseñas en /etc/shadow. Los permisos de control de acceso permiten a todo el mundo leer /etc/passwd pero sólo root puede leer las contraseñas de /etc/shadow:

*root:*1*wDASFE8ERfdferfSFgde4RFGGBSm.:12655:0:99999:7:::*
daemon::12590:0:99999:7:::*
bin::12590:0:99999:7::::*
sys::12590:0:99999:7:::*

NSS(*Name Service Switch*, Conmutación de servicio de nombres) es una biblioteca de programación en C desarrollada por Sun que fue diseñada para devolver los atributos de un objeto de usuario. En Linux y otros sistemas operativos, la configuración de NSS está controlada por el archivo *nsswitch.conf* que contiene una lista de bases de datos y orígenes. Cuando se llama a una función glibc para resolver estos tipos de objetos, se consulta cada uno de los orígenes en el orden indicado:

passwd:files
shadow:files
group:files
hosts:files

PAM *(Pluggable Authentication Module)* es un mecanismo de abstracción sencillo para la autenticación de usuarios que permite que la configuración de autenticación de cada aplicación se almacene en un archivo de configuración. Este procedimiento presenta la ventaja de que las partes que conceden privilegios de una aplicación están separados en un sistema que puede reconfigurarse finámicamente parar admitir prácticamente cualquier tipo de esquema de autenticación sin recompilar o reconfigurar la propia aplicación.
Sun Microsystems, la empresa creadora de PAM, utiliza este sistema en la versión más reciente de Solaris, ligeramente diferente en algunos aspectos respecto a la versión utilizada en este proyecto, que es la versión de Linux(compatible con todas las distribuciones modernas(Red Hat, Suse, Debian, etc...)
Cuando una aplicación necesita autenticar un usuario, llama a la función apropiada y el subsistema PAM maneja la solicitud. PAM leerá el archivo de configuración ubicado en */etc/pam.d/«nombreaplicación»*:

auth requisite pam_ nologin.so
auth required pam_ unix.so nullok
account required pam_ unix.so
session required pam_ unix.so
password required pam_ unix.so nullok obscure min=4

«nombre-servicio»: El nombre del servicio asociado(*auth.*)
«tipo-módulo»: El tipo de módulo PAM.
«indicador-control»: Controla la forma en que el módulo reaccionará.
«ruta-módulo»: La ruta relativa o absoluta al módulo
«argumentos»: Los argumentos que se pasarán al módulo

Los archivos de configuración de PAM separan las funciones de autenticación en cuatro tipos:

- auth: proporciona servicios de autenticación para establecer la identidad y conceder privilegios.
- account: gestiona los aspectos de la cuenta no relacionados con la autenticación: caducidad de la contraseña, hora del día, disponibilidad de recursos en el sistema, etc..
- session: gestiona los aspectos de una solicitud que debe llevarse a cabo antes o después de que al usuario se le conceda acceso a un servicio, este módulo realizará tareas como realizar auditorías de registro o montar/desmontar un directorio personal.

- password: un módulo password realiza la función de cambiar la contraseña del usuario.

Los indicadores de control de PAM definen la forma en la que afectará a la pila de PAM el procesamiento correcto o incorrecto de un módulo de PAM:

- requisite: un procesamiento incorrecto termina inmediatamente con el proceso de autenticación y da lugar a un fallo.
- required: un procesamiento incorrecto resultará en un fallo de autenticación, aunque se ejecutará el resto de la pila.
- sufficient: cuando el módulo se procese correctamente, la autenticación se llevará a cabo adecuadamente incluso si con anterioridad no se ha procesado correctamente un módulo required. Un procesamiento incorrecto no da lugar a fallo en la autenticación.
- optional: el procesamiento correcto o incorrecto de un módulo opcional no afectará al éxito o al fallo en la autenticación.

SAMBA

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con Linux o Mac OS X se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; a parte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.
Samba adicionalmente implementa una docena de servicios y una docena de protocolos, entre los que están NetBIOS sobre TCP/IP (NetBT), SMB (también conocido como CIFS), DCE/RPC o más concretamente, MSRPC, el servidor WINS también conocido como el servidor de nombres NetBIOS (NBNS), la suite de protocolos del dominio NT, con su Logon de entrada a dominio, la base de datos del gestor de cuentas seguras (SAM), el servicio Local Security Authority (LSA) o autoridad de seguridad local, el servicio de impresoras de NT y recientemente el Logon de entrada de Active Directory, que incluyen una versión modificada de Kerberos y una versión modificada de LDAP. Todos estos servicios y protocolos son frecuentemente referidos de un modo incorrecto como NetBIOS o SMB.

Samba configura directorios Unix/Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows, estos recursos aparecen como carpetas normales de red. Los usuarios de Linux pueden montar en sus sistemas de archivos estás

unidades de red como si fueran dispositivos locales, o utilizar la orden *smbclient* para conectarse a ellas muy al estilo del cliente de la línea de órdenes ftp Cada directorio puede tener diferentes permisos de acceso sobrepuestos a las protecciones del sistema de archivos que se esté usando en Linux.

3.4. Servicios de archivos.

El término servicios de archivos hace alusión al acceso a los archivos de un sistema remoto. Independientemente de la plataforma del equipo, la mayoría de las empresas utilizan un depósito de red para los datos a los que accede con frecuencia, incluidos los directorios principales, archivos de recursos, etc... El acceso a los datos de red debe estar protegido de un acceso no autorizado mediante un control de acceso; debe ser protegido de pérdidas o daños mediante copias de seguridad regulares y debe organizarse de una forma estructurada que facilite su expansión. A pesar de la gran diversidad de servicios de archivos disponibles en Linux, *Samba* es la solución más práctica de asistencia para los clientes de Windows con un servidor Linux.

Sistema de archivos en Windows

Los servicios de archivos ofrecen acceso de red a los datos almacenados en los sistemas de archivos. Cada tipo de sistema de archivos presenta funciones y limitaciones que inciden en la forma en que los servicios de archivos pueden compartir los datos. Los sistemas operativos modernos de Microsoft ofrecen compatibilidad local con los sistemas de archivos FAT16, FAT32, NTFS4 y NTFS5, además de la posibilidad de compartir archivos de estos sistemas de archivos en red mediante un protocolo denominado CIFS(*Common Internet File Services*). Con Windows NT4, Microsoft incluía un sistema de archivos más complejo denominado NTFS. El sistema NTFS utiliza una MFT(tabla de archivos maestra) para registrar cada archivo de la partición, con un descriptor de seguridad para cada archivo. Cada descriptor de seguridad contiene una SACL(lista de control de acceso del sistema) para auditoría y una DACL(lista de control de acceso discrecional) que incide sobre el acceso al archivo. Cada entrada de control de acceso está formada por un ID para el usuario o grupo y un permiso concedido a ese ID. Los permisos NTFS afectan directamente al acceso del sistema de archivos local y se comparan con los permisos de la ACL de compartición de archivos para determinar los accesos reales a un recurso compartido. El sistema de archivos NTFS5.0 ofrece las siguientes características:

- compatibilidad con archivos muy grandes.

- journal del sistema de archivos para auditorías.
- compatibilidad RAID
- compatibilidad con nombre de archivos de hasta 255 caracteres y diferenciación entre mayúsculas y minúsculas.
- metodología de seguridad y permisos(herencia dinámica).
- journal de cambios.
- encriptación
- compatibilidad con archivos dispersos.

Gracias a que la mayoría de las migraciones de servicios de archivos de red se hacen copiando archivos a través de la red al nuevo servidor de Linux, se hace innecesaria la utilización de un controlador NTFS para Linux.

SISTEMA DE ARCHIVOS EN LINUX

Linux admite una gran variedad de sistemas de archivos diferentes. Debido a que ext2/3 y ReiserFS son los más extendidos serán los seleccionados para la instalación del servidor Linux. Ext2/3 y ReiserFS tienen muchos atributos comunes. Cada archivo y cada directorio tienen una dirección en el disco(inodo). Ambos admiten enlaces físicos y lógicos. Cada archivo o directorio se almacena en un directorio con *"/"* o *"raíz"* en la parte superior del árbol.
El archivo de Linux */etc/fstab* contiene los sistemas de archivos, los puntos y opciones de montaje, se analiza al arrancar el sistema. Cuando se monta el sistema de archivos, se añade una línea al archivo */etc/mtab*, se lee un bit *"limpio"* en la cabecera de la partición y después, pasa a *"0"*. Cuando se desmonta, el bit limpio pasa a *"1"*. Durante el proceso de inicio, si el bit *limpio* no está en *"1"*, la partición se conoce como *sucia* y se ejecutan programas especiales para comprobar si hay errores en el sistema de archivos (*fsck, fsck.ext2 y fsck.reiserfs*).
Ext2 fue el primer sistema de archivos usado por Linux y estaba basado en Minix, posee control de acceso para lectura, escritura y ejecución, diferenciación entre mayúsculas y minúsculas, y los nombres de los archivos pueden tener hasta 255 caracteres. El principal problema de este sistema es que los ficheros pueden dañarse fácilmente con *"desmontajes sucios"*(cortes de luz, apagados incorrectos, etc...). Ext3 es un sistema de archivos Ext2 con *journaling*(un journal o registro de diario en el que se almacena la información necesaria para restablecer los datos afectados por la transacción en caso de que ésta falle).

ReiserFS organiza el sistema de archivos en dos áreas: datos y sistema. El

área está formada por directorios, archivos y metadatos de archivos, organizados como una única estructura de datos de "árbol equilibrado"(v.3) o "árbol en movimiento"(v.4). ReiserFS cuenta con el sistema de archivos más rápido, es atómico(no se producen daños en la transacción), además permite aumentar el tamaño del sistema de ficheros montado y desmontado.

3.5. Otros servicios.

Control de acceso

Los sistemas de archivo NTFS, ext2, ext3 y ReiserFS admiten control de acceso de diversas formas. Los recursos compartidos de Windows y los recursos compartidos de Samba también admiten control de acceso de diversas formas. El objetivo de la migración de Windows a Linux es mantener tantas ACL*(Control Access List)* como sea posible al mover los recursos compartidos al servidor Samba. Linux ofrece una solución para los casos en que se requieren permisos más complejos de nivel de archivo: las ACL y EA*(Extended Attributes)* POSIX añaden permisos de estilo NT a Linux, permitiendo una mayor granularidad: se pueden asignar permisos a los usuarios a nivel individual, es posible poder asignar distintos permisos basados en varios UID o GID diferentes.

4. Hoja de ruta de migración de los servicios.

4.1. Evaluación de la infraestructura actual.

El cliente en cual se basa este proyecto es el *El Consorcio Provincial de Bomberos de Valencia*, cuya infraestructura de servicios está basada en una plataforma Windows 2000 que proporciona los servicios de directorio, autenticación, DNS, DHCP y red. El cliente ha optado por migrar todos estos servicios a una plataforma GNU/Linux basada en la distribución Debian Sarge 3.1 versión *estable*, cuyo coste de licencia final es 0, frente a la opción basada en Windows Server 2003, cuyo coste es sustancialmente mayor.

4.1.1. Creación de inventario de los servidores.

La máquina objetivo de la migración y sobre la que actualmente se encuentra Windows 2000 Server es una plataforma Intel 32 bits basada en

procesador Pentium IV que actúa como PDC *(Primary Domain Controller)* sobre una red de unos 40 equipos cliente basados en diferentes tecnologías(Windows 98, 2000, XP y Linux) y ofrece servicios de archivos, autenticación, DNS y DHCP a todos los clientes de la red local. Como opción adicional en el pliego de condiciones se incluirá la configuración de un controlador de domino secundario backup(BDC), que posteriormente pueda ser utilizado en caso de fallo del controlador principal o para balanceo de carga en caso de que el crecimiento de usuarios de red pudiera saturar al controlador principal, pero este máquina no aparece en las especificaciones ni en las condiciones del proyecto.

4.1.2. Información adicional sobre la evaluación.

La descripción técnica específica de las características del hardware implicado en la migración no es determinante, los requerimientos del sistema son holgadamente suficientes y más aún teniendo en cuenta la capacidad de aprovechamiento de recursos de los sistemas Linux.

4.2. Establecimiento de los requisitos de la infraestructura Linux.

En la siguiente tabla se muestra el esquema de requisitos funcionales, está organizada en grupos de servicios de red:

Servicios	**Requisitos**
Asignación de direcciones IP	Utilizar servidor DHCP con asignación dinámica.
Resolución de nombres	Utilizar servidor DNS.
Servicios de directorio	Instalar y configurar OpenLDAP.
Migración de servicios de directorio	Migrar la información de Active Directory a OpenLDAP.
Servicios de autenticación	Instalar y configurar los servicios de autenticación de Samba.
Servicios de archivos	Instalar y configurar los servicios de archivos de Samba.
Migración de los servicios de archivos	Copiar todos los datos al nuevo servidor y establecer recursos compartidos de red.

Cuadro 3: Requisitos Funcionales

4.2.1. Creación de documentación de requisitos funcionales.

4.2.2. Establecimiento de restricciones.

La única restricción reflejada en el pliego de requerimientos es a nivel de costes e infraestructura: se empleara el mismo servidor físico original de Windows, sin realizar ninguna modificación física del hardware. Como equipo puente de pruebas se empleara otra máquina que permita almacenar temporalmente los datos de la migración y comprobar el correcto funcionamiento de los servicio migrados.

4.3. Diseño de la infraestructura Linux.

Una vez establecidos los requisitos, comienza el diseño a alto nivel de la infraestructura Linux. Es necesario determinar la estrategia global de servidores y red de la infraestructura resultante tras la migración.

4.3.1. Instalación de la plataforma.

La distribución mencionada de Debian Sarge, dispone de diversos paquetes que no son requeridos para el desarrollo del proyecto, sin embargo se ha escogido la instalación del sistema operativo en la plataforma, con el conjunto de paquetes que en el proceso de instalación se instalan automáticamente con la opción "workstation".
Los scripts diseñados para realizar las migraciones, además de los scripts que usa Samba junto con las smbldap-tools necesitan del soporte de las librerías de perl. Para obtener este soporte se han de instalar los siguientes paquetes:

apt-get install perl
apt-get install perl-base
apt-get install perl-modules
apt-get install libperl-dev
apt-get install libperl5.8

Soporte Listas Control de Acceso

Para tener el soporte de ACL (Listas de Control de Acceso) y EA (Atributo Extendidos), se han de instalar unos paquetes adicionales. Los paquetes de librería de soporte suelen estar instalados por defecto en la opción escogida de instalación de la distribución pero de todas formas se mencionan para que se tenga en cuenta que deben estar para que los ejecutables funcionen correctamente:

apt-get install libacl1
apt-get install acl
apt-get install libattr1
apt-get install attr

Una vez instalado todo lo mencionado anteriormente, ya se tienen todos los elementos necesarios para poder disfrutar de los EAs y las ACLs en los sistemas de ficheros ext2/ext3. Sólo queda un último paso, indicar al núcleo que en un determinado sistema de ficheros deseamos usar ACLs (y EAs). Para ello se debe editar el fichero /etc/fstab y añadir una opción adicional a la de aquellos sistemas de ficheros a los que queremos activar las ACLs: acl. También podemos añadir una opción para indicar explícitamente que no queremos usar las ACLs en un sistema de ficheros, aun si dicho sistema de ficheros contiene ACLs: noacl.

proc /proc proc defaults 0 0
*/dev/sda1 / ext3 defaults,**acl,user_xattr**,errors=remount-ro 0 1*
/dev/sda5 none swap sw 0 0
/dev/hdc /media/cdrom0 iso9660 ro,user,noauto 0 0
/dev/fd0 /media/floppy0 auto rw,user,noauto 0 0

Existe un juego de opciones adicional para activar o desactivar el uso de los AEs de usuario: (si hemos optado por compilarlos en nuestro núcleo) *user_xattr* y *nouser_xattr*. Por cierto, que los valores por defecto para todos los sistemas de ficheros ext2/ext3 en caso de no especificar nada son *noacl* y *nouser_xattr*. Una vez hecho lo anterior, sólo resta arrancar de nuevo el sistema y ya estan las ACLs disponibles y listas para usar.

4.4. Implantación de la infraestructura Linux.

Configuración de Openldap

La instalación y configuración de OpenLDAP se llevará a cabo de tal manera que al finalizarla, el sistema sobre el que se ha instalado debería estar listo para autentificar usuarios a través del servicio de directorios. Este es el objetivo final de este capítulo, en subsiguientes capítulos se irán añadiendo las funcionalidades necesarias para que cumpla con los requisitos del trabajo. Se ha seleccionado la versión 2.2.23-8 de OpenLDAP, que acompaña a la versión estable de Debian GNU/Linux. A lo largo de todo el documento se asume que el dominio sobre el que se ejecutará OpenLDAP es *"bombers.dva.gva.es"*. Para obtener un sistema acorde a estas condiciones, se ha añadido la línea *"bombers.dva.gva.es"* en el archivo /etc/hosts para intentar simular las condiciones reales.

El primer paso para instalar OpenLDAP, es instalar los paquetes *slapd* y *ldap-utils*. También puede ser necesario instalar las librerías de la

base de datos de LDAP *libdb4.2*:
apt-get install slapd
apt-get install ldap-utils
apt-get install libdb4.2
En la configuración se solicitará el nombre de dominio *"bombers.dva.gva.es"*, también será necesario introducir una contraseña para el administrador de Openldap y el tipo de base de datos, en (este caso hemos seleccionado *ldbm*), se opta por no eliminar la base de datos en caso de que openldap sea desinstalado.
En este punto, ya se debería tener un servidor OpenLDAP instalado y ejecutándose, aunque no esté ajustado todavía a los objetivos que persigue este apartado. Para comprobar que efectivamente el demonio slapd se está ejecutando, realizaremos un par de consultas al sistema. La primera consiste en ver si el demonio slapd se encuentra en la lista de procesos que actualmente se estén ejecutando en el sistema:

```
bombers: # ps -Af | grep slapd
root 736 1 0 18:05 ? 00:00:00 /usr/sbin/slapd
root 739 736 0 18:05 ? 00:00:00 /usr/sbin/slapd
root 740 739 0 18:05 ? 00:00:00 /usr/sbin/slapd
```

La segunda comprobación ha realizar, para ver si el demonio se está realmente ejecutando, es verificar que está escuchando en la red:

```
bombers: # netstat -puta | grep slapd
tcp 0 0 *:ldap *:* LISTEN 736/slapd
```

Una vez comprobado que el demonio slapd se está ejecutando en el sistema, se verificará que la conexión con el mismo está permitida. Para ello, se realizará una búsqueda sencilla en el directorio. Si todo va bien, se debería mostrar algo similar a:

```
bombers: # ldapsearch -x -b "" -s base '(objectclass=*)' namingContexts
# extended LDIF
#
# LDAPv3
# base <> with scope base
# filter: (objectclass=*)
# requesting: namingContexts
# # dn:
namingContexts: dc=bombers,dc=dva,dc=gva,dc=es

# search result
search: 2
result: 0 Success
```

 # numResponses: 2
 # numEntries: 1

Por defecto, el demonio slapd se ejecuta como usuario, comportamiento que no es recomendable por las implicaciones de seguridad que acarrea. En esta sección se describirán los pasos necesarios para ejecutar el demonio slapd con un usuario un grupo específicos. Antes de poder ejecutar el demonio slapd con un usuario y grupo específico, se ha de crear el usuario y grupo en el sistema, en caso de no existir. El tipo de usuario grupo que se crearán son los llamados "de sistema", y se denominarán "slapd":

bombers: # addgroup –-system slapd
Adding group 'slapd' (111)...
Hecho.
bombers: # adduser —home /var/lib/ldap/ –-shell /bin/false —no-create-home –-ingroup slapd —system slapd
Añadiendo usuario del sistema slapd...
Adding new user 'slapd' (105) with group 'slapd'.
No se crea el directorio home.

La carpeta "home" del usuario slapd es el directorio /var/lib/ldap (donde se almacena la base de datos de OpenLDAP, entre otras cosas), no posee shell asociado y está dentro del grupo slapd que se acaba de crear.
Antes de continuar, se ha de parar el demonio slapd para evitar comportamiento no deseado:

bombers: # /etc/init.d/slapd stop
Stopping OpenLDAP: slapd.

Antes de ejecutar el demonio slapd con el nuevo usuario y grupo creados, es necesario cambiar el propietario y el grupo de algunos archivos y directorios relacionados con slapd, para que este funcione con normalidad. Los cambios han de realizarse en los siguientes directorios, así como en los archivos que albergan:

debian: # chown -R slapd.slapd /etc/ldap/ /var/lib/ldap/ /var/lib/slapd/ /var/run/slapd/

El último paso consiste en indicar al demonio slapd con qué usuario y grupo se ha de ejecutar a partir de ahora. Esta característica se configura asignando los valores correspondientes a las variables *SLAPD_USER* y *SLAPD_GROUP* del archivo */etc/default/slapd*:

SLAPD_USER=slapd

SLAPD_GROUP=slapd

Ahora sólo queda arrancar de nuevo el demonio slapd para que se ejecute con el nuevo usuario:

debian: # /etc/init.d/slapd start
debian: # ps auxf | grep slapd
slapd 937 0.0 1.6 11276 3228 ? Ss 11:10 0:00 /usr/sbin/slapd -g slapd -u slapd

Configuración cliente Openldap, archivo /etc/ldap/ldap.conf

El archivo de configuración global empleado por los clientes LDAP se encuentra en /etc/ldap/ldap.conf y es necesario especificar las líneas:

HOST 127.0.0.1
BASE dc=bombers,dc=dva,dc=gva,dc=es
nss_base_passwd ou=Users,dc=bombers,dc=dva,dc=gva,dc=es?sub
nss_base_passwd ou=Computers,dc=bombers,dc=dva,dc=gva,dc=es?sub
nss_base_shadow ou=Users,dc=bombers,dc=dva,dc=gva,dc=es?sub
nss_base_group ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es?sub
ssl no
pam_password ssha

Ha de asegurarse que los permisos de este archivo estén bien asignados (se ha de leer por todo el mundo):

-rw-r–r– 1 slapd slapd 344 2006-10-31 11:20 /etc/ldap/ldap.conf

Configuración servidor Openldap, archivo /etc/ldap/slapd.conf

Se ha de realizar un cambio de permisos, de forma que sólo el propietario tenga permisos de lectura y escritura:

debian: # chmod -v 0600 /etc/ldap/slapd.conf
el modo de «/etc/ldap/slapd.conf» cambia a 0600 (rw——-)

A continuación añadiremos el usuario administrador del ldap, mediante dos líneas en el archivo */etc/ldap/slapd.conf*:

rootdn "cn=admin,dc=bombers,dc=dva,dc=gva,dc=es"
rootpw {SSHA}G05D97jB8KkfKoGpRKJvbkbJnTR14Wx6

En la primera línea indicamos el DN(distinguised name) del usuario administrador y en la segunda línea indicamos su password encriptado, que hemos obtenido anteriormente con el comando:
debian: # slappasswd -h SSHA -s damarsan
{SSHA}G05D97jB8KkfKoGpRKJvbkbJnTR14Wx6

Para que las búsquedas sobre el directorio LDAP sean más rápidas, han sido declarados índices en el fichero de configuración slapd.conf, ejecutaremos una reindexación de la base de datos del directorio como se describe a continuación:

indices añadidos al fichero de configuración:
index objectClass,uidNumber,gidNumber eq
index cn,sn,uid,displayName pres,sub,eq
index memberUid,mail,givenName eq,subinitial
index sambaSID,sambaPrimaryGroupSID,sambaDomainName eq
reindexación:
debian: # slapindex -vf /etc/ldap/slapd.conf
indexing id=00000001
indexing id=00000002
debian: # /etc/init.d/slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: (db4.2_recover not found), slapd.

Para proteger los datos confidenciales del directorio(passwords, etc..) añadiremos las siguientes líneas al fichero de configuración(sólo el propietario de los atributos tiene permisos sobre éstos):

access to attrs=userPassword,sambaLMPassword,sambaNTPassword
by self write
by anonymous auth
*by * none*

Configuración de autenticación PAM

En este capítulo se verá como configurar una máquina para que sus usuarios se autentiquen a través de un servidor LDAP. Para ello se han de modificar dos aspectos del comportamiento del sistema: El mapeado entre los números de identificación de los usuarios y sus nombres (utilizados, por ejemplo, por /bin/ls -l) o la localización del directorio *home*. La búsqueda de este tipo de información es responsabilidad del servicio de nombres cuyo archivo de configuración es: */etc/nsswitch.conf*. La autenticación (comprobación de claves), que es responsabilidad del subsistema PAM, cuya configuración se hace a través del directorio /etc/pam.d/. Ambos subsistemas se han de configurar

separadamente, pero en este caso ambos se van a configurar de tal forma que hagan uso de LDAP.

Antes de poder autentificar a los usuarios a través de un servidor LDAP, es necesario instalar algunas utilidades en el cliente, como *pam_ldap y nss_ldap*. El paquete *pam_ldap* permite hacer uso de un servidor LDAP para la autenticación de usuarios (comprobación de claves) a aquellas aplicaciones que utilicen PAM. En Debian GNU/Linux el paquete libpam-ldap provee esta funcionalidad, por lo que será instalado en la máquina como se muestra a continuación:

debian: # apt-get install libpam-ldap

- En servidor LDAP indicaremos la IP privada de la máquina: 192.168.0.8
- El nombre distintivo (DN) especificaremos el nombre del dominio en terminología ldap *dc=bombers,dc=dva,dc=gva,dc=es*.
- Seleccionaremos la versión 3 de ldap.
- Contestamos afirmativamente a esta pregunta, de esta forma, aquellas aplicaciones que cambien claves por medio de PAM, se comportarán como si lo hiciesen de forma local.
- Indicaremos que no se necesite login para realizar consulta a la base de datos de la ldap.
- Especificaremos el DN del administrador de LDAP: cn=admin,-dc=bombers,dc=dva,dc=gva,dc=es y el password.
- Por último, el método de encriptación elegido para almacenar las claves ha sido "exop", de esta forma pam-ldap utilizará el algoritmo de hash especificado en el archivo /etc/ldap/slapd.conf, en lugar de realizar la operación hash localmente y escribir el resultado en la base de datos directamente.
- Es necesario asignar permisos de lectura a todos los usuarios del sistema al archivo de configuración generado:
  debian: # chmod -v 644 /etc/pam_ldap.conf
  el modo de «/etc/pam_ldap.conf» cambia a 0644 (rw-r–r–)

El paquete *libnss-ldap* permite a un servidor LDAP actuar como un servidor de nombres. Esto significa que provee la información de las cuentas de usuario, los IDs de los grupos, la información de la máquina, los alias, los grupos de red y básicamente cualquier cosa que normalmente se obtiene desde los archivos almacenados bajo /etc o desde un servidor NIS. En Debian GNU/Linux el paquete libnss-ldap provee esta funcionalidad, por lo que será

instalado en la máquina como se muestra a continuación:

debian: # apt-get install libnss-ldap

En la pantalla de configuración introduciremos los siguiente parámetros:

- En servidor LDAP indicaremos la IP privada de la máquina: 192.168.0.8
- El nombre distintivo (DN) especificaremos el nombre del dominio en terminología ldap *dc=bombers,dc=dva,dc=gva,dc=es*.
- Seleccionaremos la versión 3 de ldap.
- Indicaremos que no se necesite login para realizar consulta a la base de datos de la ldap.
- Otorgaremos permisos de lectura a todos los usuarios no sólo al propietario al archivo */etc/libnss-ldap.conf*:
  -rw-r–r– 1 root root 9121 2006-10-31 12:25 /etc/libnss-ldap.conf

Una vez finalizada la configuración es imprescindible añadir las siguientes líneas al archivo de configuración *libnss-ldap.conf*:

binddn cn=admin,dc=bombers,dc=dva,dc=gva,dc=es
bindpw SSHAG05D97jB8KkfKoGpRKJvbkbJnTR14Wx6

Mediante estas líneas permitiremos que la librería libnss pueda contactar con ldap, indicando el DN del administrador de ldap y su password encriptado.

Configuración de Nsswitch

nsswitch.conf es el fichero de configuración de las Bases de Datos del Sistema y del sistema de Conmutación de los Servicios de Nombres (Name Service Switch).
En otras palabras, es un archivo que indica el orden y el procedimiento a seguir para la búsqueda de la información requerida, por ejemplo, para hacer búsquedas de hosts o usuarios. La forma de configurar este archivo es muy simple: primero se especifica la base de datos sujeta a la búsqueda (primera columna) seguida del procedimiento que se va a emplear para realizar una búsqueda sobre la misma (columnas siguientes).
De esta forma, basta con configurar el procedimiento de búsqueda para que haga uso de LDAP en algún momento:

#/etc/nsswitch.conf
#
 # Example configuration of GNU Name Service Switch functionality.

 # If you have the 'glibc-doc' and 'info' packages installed, try:
 # 'info libc "Name Service Switch"' for information about this file.

passwd: files ***ldap*** *compat*
group: files ***ldap*** *compat*
shadow: files ***ldap*** *compat*

hosts: files ***ldap*** *dns*
networks: files

protocols: db files
services: db files
ethers: db files
rpc: db files

netgroup: files ***ldap*** *nis*

Hay que destacar que no se ha eliminado el uso de los ficheros locales, "files", ya que algunos usuarios y grupos de usuarios (como por ejemplo root) permanecerán de forma local. Si el sistema no utiliza la entrada "files", y el servidor LDAP se cae, nadie, ni siquiera root, podrá entrar al sistema. Es recomendable que solo exista la cuenta de root como local (files) y el resto de cuentas de usuario sean definidas en el directorio LDAP.

PAM permite configurar el método de autenticación que van a utilizar las aplicaciones que hagan uso de él. Gracias a esto, se pueden añadir fácilmente distintas opciones de autenticación, como el uso de una base de datos LDAP. En las siguientes secciones se mostrarán los archivos que se han de modificar para lograr la autenticación a través de LDAP. Hace relativamente poco tiempo que la versión estable de Debian (Sid) ha cambiado la forma de configuración de PAM. Actualmente posee secciones comunes a todos los archivos, estas secciones comunes son aquellos archivos localizados en el directorio /etc/pam.d/ que comiencen por "common-". pam-ldap asume que las cuentas del sistema son objetos con los siguientes atributos: *uid y userPassword*. Los atributos están permitidos por la clase objeto (objectClass) *posixAccount*.
A continuación se detalla las modificaciones a realizar en los archivos indicados:

- **etc/pam.d/common-account:**
  account sufficient pam_ldap.so debug
  account required pam_unix.so

- **etc/pam.d/common-auth:**
  auth sufficient pam_ldap.so use_first_pass debug
  auth required pam_unix.so nullok_secure

- **etc/pam.d/common-session:**
  session required pam_unix.so
  session optional pam_ldap.so debug

- **etc/pam.d/common-passwd:**
  password sufficient pam_ldap.so
  password required pam_unix.so nullok obscure min=4 max=8 md5 use_first_pass

Consultando en apartados anteriores, concretamente en el apartado 3.3 *Servicios de autenticación* comprobamos que se ha optado por utilizar la opción *sufficient* para evitar que aunque se produzca fallo en la autenticación de ldap permita el acceso al sistema de usuarios locales(sobre todo root).

Configuración de SAMBA

El servidor Samba se instalará y configurará para que actúe como PDC de la red local en la que esté presente. La información de las cuentas de los usuarios se almacenará en un directorio LDAP. Una vez se haya incorporado esta estructura en el directorio LDAP, los usuarios que ahí se almacenen tendrán la posibilidad de autenticarse en cualquier sistema GNU/Linux y/o Windows que haga uso del servidor LDAP para la autenticación de usuarios. La particularidad es que tendrán la misma cuenta de acceso para los todos sistemas, tanto en GNU/Linux como en Windows, de toda la red. Se ha de diferenciar la instalación de un servidor Samba de la instalación de un cliente. En las siguientes secciones se verá como instalar uno y otro, así como los requisitos para que todo funcione correctamente. En muchas ocasiones un mismo ordenador puede actuar como cliente y servidor Samba. En esta documentación se entenderá por servidor Samba, aquel ordenador que preste servicios (autenticación, compartición de unidades y archivos, etc.), y un cliente será aquel que los utilice (acceso a los recursos compartidos, autenticación, montaje de sistemas de archivos compartidos, etc.).

En primer lugar, realizaremos la instalación del paquete samba:

debian: # apt-get install samba

En la pantalla de configuración introduciremos los siguientes parámetros:

- El nombre del dominio o grupo de trabajo sera: *BOMBERS*

- Se utilizarán contraseñas cifradas para permitir la compatibilidad con clientes Windows.

- El servidor no recibe la dir. IP desde un servidor DHCP, por lo que no leeremos la configuración WINS.
- Ejecutaremos SAMBA como demonio independiente.
- Creamos el archivo de contraseñas cifradas */var/lib/samba/passdb.tdb*

Hay dos paquetes importantes para un cliente Samba: *smbclient* y *smbfs* que dependen del paquete *samba-common*, al igual que el paquete *samba*:

debian: # apt-get install smbclient smbfs

Una vez se ha completado el proceso de instalación, el sistema tendrá disponibles las siguientes herramientas (para saber que hace cada una, se pueden consultar las páginas del manual que traen adjuntas):

debian: # dpkg -L smbclient | grep bin
/usr/bin
/usr/bin/smbclient
/usr/bin/smbtar
/usr/bin/rpcclient
/usr/bin/smbspool
/usr/bin/smbtree
/usr/bin/smbcacls
/usr/bin/smbcquotas

debian: # dpkg -L smbfs | grep bin
/sbin
/sbin/mount.cifs
/usr/bin
/usr/bin/smbmount
/usr/bin/smbumount
/usr/bin/smbmnt
/sbin/mount.smbfs
/sbin/mount.smb

Antes de continuar con la configuración de Samba, es necesario realizar algunas modificaciones y ajustes en la configuración de OpenLDAP, de forma que quede preparado para soportar las características de Samba. Se deberá copiar el esquema de samba al directorio de esquemas de OpenLDAP que se encuentra en el paquete samba-doc, por lo que si no ha sido instalado en el sistema previamente, deberá ser instalado:

debian: # apt-get install samba-doc
debian: # cp /usr/share/doc/samba-doc/examples/LDAP/sambaṡchemaġz-
debian: # gunzip -v /etc/ldap/schema/samba.schema.gz

debian: # chown -v slapd.slapd /etc/ldap/schema/samba.schema
cambiado el propietario de «/etc/ldap/schema/samba.schema» a slapd:slapd
debian: # chmod -v 644 /etc/ldap/schema/samba.schema
el modo de «/etc/ldap/schema/samba.schema» cambia a 0644 (rw-r–r–)

En el fichero de configuración del servidor ldap (*/etc/ldap/slapd.conf*) es necesario añadir la siguiente línea, que hace referencia al esquema de objetos pertenecientes a Samba:

include /etc/ldap/schema/samba.schema

La configuración de Samba se almacena en el archivo *smb.conf*, que en el sistema Debian GNU/Linux se encuentra en el directorio /etc/samba/. En esta sección se configurará Samba como un Controlador Primario de Dominio que almacena su base de datos SAM en un servidor OpenLDAP. Para la configuración se asumirá que:

- El nombre del dominio será: BOMBERS
- El nombre del servidor Netbios será: DEBIAN
- El directorio por defecto *home* de los usuarios estará en: */home/usuarios/NOMBREUSUARIO*
- Los perfiles móviles por defecto se almacenarán en: */home/profiles/NOMBREUSUARIO*

os datos principales que deben aparecer en el archivo de configuración en la sección *[global]* que contiene los parámetros generales del servidos Samba son:

- *workgroup = BOMBERS*
- *netbiosname = DEBIAN*
- *server string = %h Servidor SAMBA-LDAP PDC (Samba %v)*
- *enable privileges = Yes*
- *ldap passwd sync = Yes*
- *passdb backend = ldapsam:ldap://127.0.0.1/*
- *ldapadmindn=cn=admin,dc=bombers,dc=dva,dc=gva,dc=es*
- *ldap group suffix = ou=Groups*
- *ldap machine suffix = ou=Computers*
- *ldap user suffix = ou=Users*

- *dos charset = 850*
- *unix charset = ISO8859-1*
- *add user script = /usr/local/sbin/smbldap-useradd -a '%u'*
- *delete user script = /usr/local/sbin/smbldap-userdel '%u'*
- *add group script = /usr/local/sbin/smbldap-groupadd -p '%g'*
- *delete group script = /usr/local/sbin/smbldap-groupdel '%g'*
- *add group script = /usr/local/sbin/smbldap-groupadd -p '%g'*
- *delete group script = /usr/local/sbin/smbldap-groupdel '%g'*
- *add user to group script = /usr/local/sbin/smbldap-groupmod -m '%u' '%g'*
- *delete user from group script = /usr/local/sbin/smbldap-groupmod -x '%u' '%g'*
- *set primary group script = /usr/local/sbin/smbldap-usermod -g '%g' '%u'*
- *add machine script = /usr/local/sbin/smbldap-useradd -w -i '%u'*
- *domain logons = Yes*
- *preferred master = Yes*
- *wins support = Yes*
- *ldap admin dn = cn=admin,dc=bombers,dc=dva,dc=gva,dc=es*
- *idmap backend = ldap:ldap://debian.bombers.dva.gva.es/*

En el apartado *share definitions* incluiremos todos las carpetas de red que van a ser utilizadas por los usuarios:

[homes]
comment = Directorios Home
valid users = %U
create mask = 0700
directory mask = 0700
browseable = No

[netlogon]
comment = Network Logon Service
path = /home/netlogon

write list = root
browseable = No

[F]
path = /home
read only = No
profile acls = Yes

[profiles]
path = /home/profiles
force user = %U
read only = No
create mask = 0600
directory mask = 0700
guest ok = Yes
browseable = No
csc policy = disable

A continuación hay que crear los directorios que utilizaremos como recursos compartidos:
debian: # mkdir /home/netlogon
debian: # mkdir /home/profiles
Para que todos los usuarios tengan acceso a este recursos modificaremos los permisos asignados:
debian: # chmod 1777 /home/profiles

Instalación y configuración de SMBLDAP-TOOLS

Las herramientas que provee el paquete smbldap-tools, son un conjunto de scripts que se ejecutan sobre las herramientas de sistema: useradd, userdel y usermod y groupadd, groupdel y groupmod, para permitir la manipulación de usuarios y grupos almacenados en el directorio LDAP, destinadas a sistemas DEN como Samba-LDAP y pam/nss_ldap.
La última versión de estas herramientas se encuentra en: *http://samba.idealx.org*. La versión utilizada ha sido la 0.9.1.

Los scripts que provee el conjunto de herramientas smbldap-tools necesitan el paquete *libnet-ldap-perl*, por lo que si no se encuentra instalado en el sistema, se debe ejecutar:

debian: # apt-get install libnet-ldap-perl

Una vez descargado el fichero *smbldap-tools-0.9.1.tgz*, realizaremos la instalación de las herramientas:

debian:/tmp# tar -zxvf smbldap-tools-0.9.1.tgz
debian:/tmp# chown root.root -R smbldap-tools-0.9.1
debian:/tmp# cp -v –remove-destination smbldap-tools-0.9.1/smbldap- smbldap-tools-0.9.1/smbldap*.pm /usr/local/sbin/*
debian:/tmp# mkdir -vm 755 /etc/smbldap-tools
mkdir: se ha creado el directorio «/etc/smbldap-tools»
*debian:/tmp# cp smbldap-tools-0.9.1/smbldap*conf /etc/smbldap-tools/*
*debian:/tmp# chmod -v 600 /etc/smbldap-tools/**
el modo de «/etc/smbldap-tools/smbldap_bind.conf» cambia a 0600 (rw——-)
el modo de «/etc/smbldap-tools/smbldap.conf» cambia a 0600 (rw——-)

Una ver realizada la instalación, ejecutaremos el script que solicitará los parámetros necesarios para la configuración, para seleccionar las opciones que aparecen por defecto(entre paréntesis) pulsaremos *enter*:

debian:/tmp/smbldap-tools-0.9.1# ./configure.pl
-=
smbldap-tools script configuration
-=
Looking for configuration files...
Samba Configuration File Path [/etc/samba/smb.conf]
The default directory in which the smbldap configuration files are stored is shown.
If you need to change this, enter the full directory path, then press enter to

continue.
Smbldap-tools Configuration Directory Path [/etc/smbldap-tools/] >
-=-
=-=-=-=-=
Let's start configuring the smbldap-tools scripts ...

. workgroup name: name of the domain Samba act as a PDC
workgroup name [BOMBERS] >
. netbios name: netbios name of the samba controler
netbios name [DEBIAN] >
logon drive [] >
. logon home: home directory location (for Win95/98 or NT Workstation).
(use %U as username) Ex:'\\DEBIAN\ %U'
logon home (press the "." character if you don't want homeDirectory)[\\DEBIAN\ %U] >
. logon path: directory where roaming profiles are stored. Ex:\\DEBIAN\profiles\ %U
logon path (press the "." character if you don't want roaming profile) [\\DEBIAN\profiles\ %U] >
. home directory prefix (use %U as username) [\home\ %U] >
. default users' homeDirectory mode [700] >
. default user netlogon script (use %U as username) [] >
default password validation time (time in days) [45] >
. ldap suffix [dc=bombers,dc=dva,dc=gva,dc=es] >
. ldap group suffix [ou=Groups] >
. ldap user suffix [ou=Users] >
. ldap machine suffix [ou=Computers] >
. Idmap suffix [ou=Idmap] >
sambaUnixIdPooldn object (relative to $suffix) [sambaDomainName=BOMBERS] >
ldap master server [127.0.0.1] > debian.bombers.dva.gva.es
. ldap master port [389] >
. ldap master bind dn [cn=admin,dc=bombers,dc=dva,dc=gva,dc=es] >
. ldap master bind password [] >
ldap slave server [127.0.0.1] >
. ldap slave port [389] >
. ldap slave bind dn [cn=admin,dc=bombers,dc=dva,dc=gva,dc=es] >
. ldap slave bind password [] >
. ldap tls support (1/0) [0] >
. SID for domain BOMBERS: SID of the domain (can be obtained with 'net getlocalsid DEBIAN')
SID for domain BOMBERS[S-1-5-21-658922739-2820689373-2813278431]>
. unix password encryption: encryption used for unix passwords
unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA) [SSHA] >

. default user gidNumber [513] >
. default computer gidNumber [515] >
. default login shell [/bin/bash] >
. default skeleton directory [/etc/skel] >
. default domain name to append to mail adress [] >
-=-
backup old configuration files:
/etc/smbldap-tools/smbldap.conf->/etc/smbldap-tools/smbldap.conf.old
/etc/smbldap-tools/smbldap_bind.conf->/etc/smbldap-tools/smbldap_bind.conf.old
writing new configuration file:
/etc/smbldap-tools/smbldap.conf done.
/etc/smbldap-tools/smbldap_bind.conf done.

La configuración se almacena en dos archivos: */etc/smbldap-tools/smbldap.conf*, que contiene los datos de configuración relativos a Samba, y el archivo */etc/smbldap-tools/smbldap_bind.conf* que contiene los datos de la cuenta de administrador de LDAP al que únicamente puede acceder el usuario root.
Una vez realizada la configuración y planificada la estructura DN del ldap se modificará el fichero */etc/libnss-ldap.conf* agregando las siguientes líneas:

rootbinddn cn=admin,dc=bombers,dc=dva,dc=gva,dc=es
binddn cn=admin,dc=bombers,dc=dva,dc=gva,dc=es
bindpw {SSHA}G05D97jB8KkfKoGpRKJvbkbJnTR14Wx6
nss_base_passwd ou=Users,dc=bombers,dc=dva,dc=gva,dc=es?sub
nss_base_passwd ou=Computers,dc=bombers,dc=dva,dc=gva,dc=es?sub
nss_base_shadow ou=Users,dc=bombers,dc=gva,dc=dva,dc=es?sub
nss_base_group ou=Groups,dc=bombers,dc=gva,dc=dva,dc=es?sub
nss_base_hosts ou=Computers,dc=bombers,dc=dva,dc=gva,dc=es?sub

la primera línea indica el DN(*distinguished name*) para agregar equipos al servidor, cuyo pasword debe almacenarse en formato plano en el archivo */etc/ldap.secret*, al que sólo tendrá acceso el usuario root. Las siguientes líneas indican la estructura de búsqueda de las OU(*unidades organizativas*
Para realizar una primera carga del directorio de OpenLDAP, se usa el ejecutable de *smbldap-tools* denominado *smbldap-populate*, que crea la estructura necesaria para la migración, además de los usuarios *nobody* y el administrador del dominio, cuyo nombre es pasado como opción de la siguiente forma:
(El script *smbldap-populate* requiere los paquetes de perl *libcrypt-smbhash-perl* y libdigest-sha1-perl que instalaremos antes de ejecutar el script)

debian:/opt/smbldap-tools-0.9.1# apt-get install libcrypt-smbhash-perl libdigest-sha1-perl

A continuación ejecutaremos el script utilizando como parámetros el nombre usuario Administrador del directorio:

debian:/opt/smbldap-tools-0.9.1# ./smbldap-populate -a Administrador

Populating LDAP directory for domain BOMBERS (S-1-5-21-658922739-2820689373-2813278431) (using builtin directory structure)

entry dc=bombers,dc=dva,dc=gva,dc=es already exist.
adding new entry: ou=Users,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: ou=Computers,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: ou=Idmap,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: uid=Administrador,ou=Users,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: uid=nobody,ou=Users,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Domain Admins,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Domain Users,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Domain Guests,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Domain Computers,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Administrators,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Account Operators,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Print Operators,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Backup Operators,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: cn=Replicators,ou=Groups,dc=bombers,dc=dva,dc=gva,dc=es
adding new entry: sambaDomainName=BOMBERS,dc=bombers,dc=dva,dc=gva,dc=es

Please provide a password for the domain Administrador:
Changing password for Administrador
New password :
Retype new password :

Una vez se ha cargado la estructura básica, comprobaremos que los datos de creación son correctos mediante el uso de la herramienta freeware *ldap-browser*, que previamente hemos configurado con los parámetros de nuestro servicio de directorio:

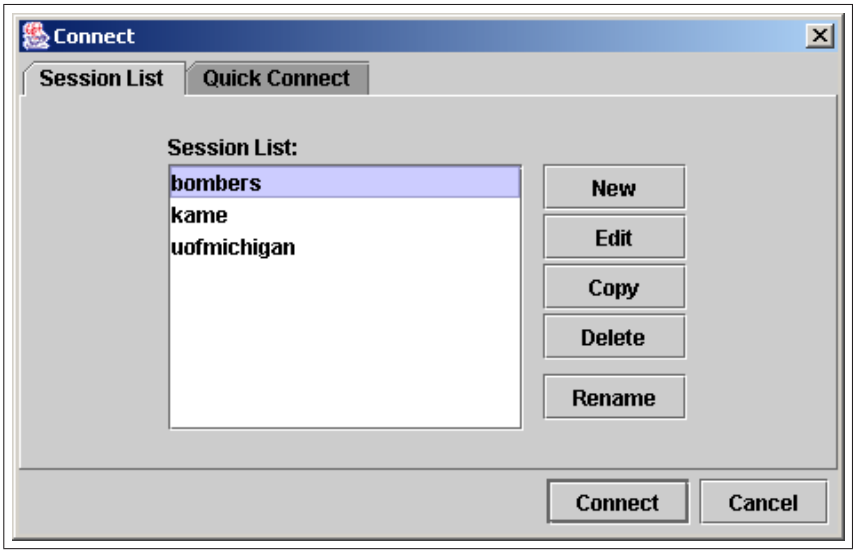

Figura 4: Conexión con GUI al servicio de directorio

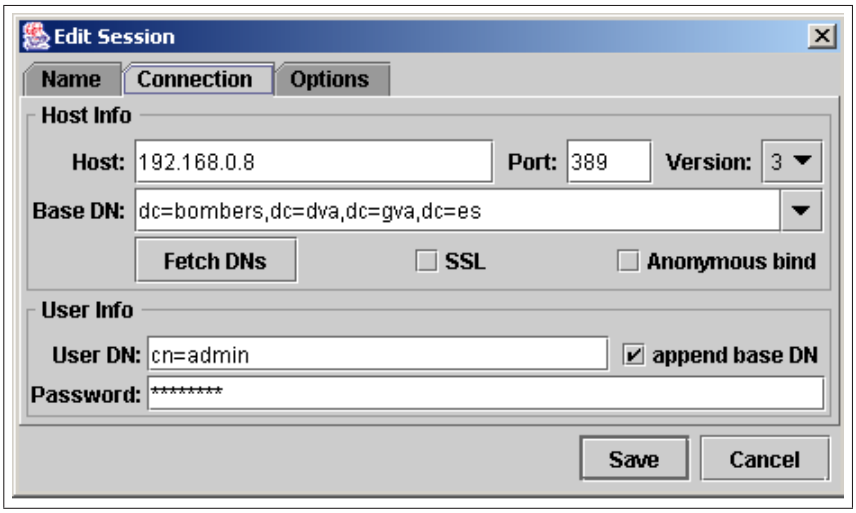

Figura 5: Conexión con GUI al servicio de directorio

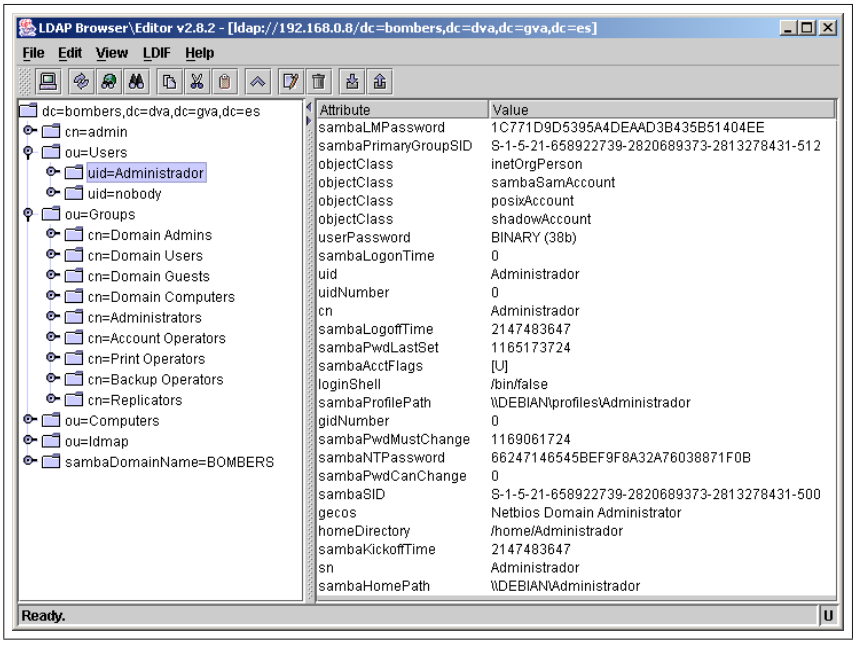

Figura 6: Estructura creada con smbldap-tools

Ahora que ya está el sistema preparado para hacer uso de LDAP en la autenticación de los usuarios, sería recomendable hacer algunas pruebas con la nueva configuración para ver si todo funciona correctamente.
El comando *pamtest* acepta dos parámetros: el primero es el nombre del servicio al cual se va a conectar para realizar la autenticación, el segundo es el nombre del usuario que se va a autentificar sobre dicho servicio. El comando pamtest se encuentra en el paquete *libpam-dotfile*, por lo que si no está disponible en el sistema, ha de ejecutarse:

debian: # apt-get install libpam-dotfile

Una vez instalado el paquete podemos comprobar que el servicio funciona correctamente creando una cuenta en el ldap y ejecutando pamtest:

debian: # smbldap-useradd -m testuser
debian: # smbldap-passwd testuser
Changing password for testuser
New password :
Retype new password :
debian: # getent passwd | grep testuser
testuser:x:1014:513:System User:/home/testuser:/bin/bash
debian: # pamtest passwd testuser
Trying to authenticate <testuser> for service <passwd>.
Password:

Authentication successful.

Configuración políticas de seguridad

Para la gestión de políticas de seguridad en Samba, se utiliza el comando *pdbedit*, con la siguiente opción se muestran las políticas que Samba soporta:

debian: # pdbedit -P ?
No account policy by that name
Account policy names are :
min password length
password history
user must logon to change password
maximum password age
minimum password age
lockout duration
reset count minutes
bad lockout attempt
disconnect time
refuse machine password change

- min password length: Especifica el tamaño mínimo de caracteres que debe tener una contraseña.
- password history: se indica el número de contraseñas que Samba debe recordar para que el usuario no las repita al cambiar su contraseña.
- user must logon to change password: obliga al usuario a entrar en el sistema si desea cambiar su contraseña.
- maximum password age: indica la cantidad de días que una contraseña es válida y cuando se cumple el plazo de validez, obliga al usuario a que la cambie.
- minimum password age: indica la cantidad de días que una contraseña debe permanecer activa antes de que el usuario pueda cambiarla.
- bad lockout attempt: especifica el número de veces que un usuario puede equivocarse de contraseña, una vez sobrepasado ese contador, la cuenta es bloqueada.
- lockout duration: establece la cantidad de minutos que una cuenta de usuario permanecerá bloqueada después de cumplir la condición especificada en bad lockout attempt.

- reset count minutes: tiempo en minutos que espera para resetear el contador de intentos de logon fallidos, siempre y cuando este contador no haya alcanzado el numero especificado en bad lockout attempt.
- disconnect time: establece un tiempo en minutos de desconexión de usuario por inactividad.
- refuse machine password change: indica si se puede o no cambiar la contraseña de maquina o computadora.

Los valores pasados a las políticas se establecen con la opción "−C", y se especifican los valores de desactivación de políticas con "−1" si se trata de tiempo y "0" si se trata de cantidad. Excepto para la política de "minimum password age" que la desactivación sería "0", ya que la indicar "−1" supondría que la contraseña nunca se puede cambiar.
Un ejemplo de configuración de políticas sería el que se muestra a continuación:

debian: # pdbedit -P "min password length" -C 5
account policy value for min password length was 8
account policy value for min password length is now 5
debian: # pdbedit -P "password history" -C 4
account policy value for password history was 0
account policy value for password history is now 4
debian: # pdbedit -P "maximum password age" -C 90
account policy value for maximum password age was 4294967295
account policy value for maximum password age is now 90
debian: # pdbedit -P "minimum password age" -C 7
account policy value for minimum password age was 0
account policy value for minimum password age is now 7
debian: # pdbedit -P "bad lockout attempt" -C 8
account policy value for bad lockout attempt was 0
account policy value for bad lockout attempt is now 8
debian: # pdbedit -P "lockout duration" -C 1
account policy value for lockout duration was 30
account policy value for lockout duration is now 1

Configuración DNS y DHCP

En la red del Consorcio Provincial de Bomberos de Valencia se dispone de equipos configurados con una IP fija y otros configurados con la obtención de esta de forma dinámica.
Cuando es añadido un equipo nuevo a la red con un nombre nuevo a la red y este obtiene su dirección IP mediante DHCP es tarea del administrador de la red añadir al DNS la nueva referencia de nombre de equipo para que sea detectado dentro de la red interna.
Las presentes configuraciones de DNS y DHCP hacen esta parte dinámica de forma que cuando un equipo nuevo entra en la red y obtiene su nueva dirección IP se actualicen solos los registros de DNS y no tenga que intervenir el administrador.
De la misma forma cuando el equipo se desconecte de la red o se apague tras un espacio de tiempo las tablas de DNS son actualizadas eliminando la entrada.
Para habilitar el servidor DNS es necesario instalar el paquete *bind9*:

debian: # apt-get install bind9

Para habilitar el servidor DHCP, son necesarios los siguientes paquetes:

debian: # apt-get install dhcp3-common
debian: # apt-get install dhcp3-server

En la pantalla de configuración es necesario introducir los siguientes parámetros:
La interfaz de red por la cual responderá el servidor, en este caso:*eth0*
En primer lugar realizaremos la configuración del servidor DNS:
Básicamente deberemos modificar el fichero de configuración del DNS */etc/bind/named.conf.local* donde indicamos los ficheros de zona que utilizamos.

```
zone "bombers.dva.gva.es" {
type master;
file "/etc/bind/db.bombers.dva.gva.es";
allow-query { any; };
allow-update { localnets; key rndc-key; };
notify no;
};

zone "0.168.192.in-addr-arpa" {
type master;
file "/etc/bind/db.192.168.0";
allow-query { any; };
allow-update { localnets;key rndc-key; };
```

notify no;
};

En el cual indicamos las zonas locales tanto directa como inversa. A su vez para cada zona indicamos que puede realizar consultas al DNS *allow-query {any;};* y quien puede modificar el contenido del mismo. *allow-update { localnets, key mdc- key; };*.
Con esta ultima directiva se indica que solo puedan realizar actualizaciones de las entradas del DNS los equipos de la red local y que lo hagan de forma encriptada utilizando la clave *rndc.key*, obtenida mediante el comando *rndc-confgen -a* y que copiaremos en */etc/bind/named.conf.options:*

key "rndc-key" {
algorithm hmac-md5;
secret "wr8Rfj1PbLQbTaGs2qkMCQ==";
};
controls {
inet 127.0.0.1
allow {localnets; } keys { rndc-key; };
};

A continuación realizaremos la configuración manual editando el archivo */etc/dhcp3/dhcpd.conf*:

server-identifier debian.bombers.dva.gva.es;
#clave de encriptación
include "/etc/bind/rndc.key"; };
ddns-update-style interim;
 # option definitions common to all supported networks...
option domain-name "bombers.dva.gva.es";
option domain-name-servers 192.168.0.8;
ddns-updates on;
ddns-domainname "bombers.dva.gva.es";
default-lease-time 600;
max-lease-time 7200;
 # If this DHCP server is the official DHCP server for the local
 # network, the authoritative directive should be uncommented.
***authoritative**;*
subnet 192.168.0.0 netmask 255.255.255.0 {
one-lease-per-client on;
option routers 192.168.0.254;
range 192.168.0.11 192.168.0.21;
}
zone bombers.dva.gva.es. {

primary 127.0.0.1;
key rndc-key;
}

zone 0.168.192.in-addr-arpa. {
primary 127.0.0.1;
key rndc-key;
}

A continuación se describen los parámetros principales de configuración del servidor DHCP:

- ⇨ *server-identifier*: identificador del servidor DHCP, que en este caso coincide con la máquina local.
- ⇨ *include "/etc/bind/rndc.key"*: incluimos el archivo con la clave, para que el servidor pueda autenticarse con bind9.
- ⇨ *ddns-update-style interim;*: esta línea indica el método de actualización DNS automática con los valores de la IP asignados por DHCP.
- ⇨ *option domain-name "bombers.dva.gva.es";*: definimos el nombre del dominio DNS que se añade a los nombres de host.
- ⇨ *option domain-name-servers 192.168.0.8;*: definimos la dirección del servidor DNS de la red, que en este caso coincide con la máquina local.
- ⇨ *ddns-domainname "bombers.dva.gva.es";*: indica el dominio en el que se actualizan los DNS.
- ⇨ *default-lease-time 600;*: indica el tiempo de asignación de IP en segundos.
- ⇨ *max-lease-time 7200;*: indica el tiempo máximo de asignación en segundos.
- ⇨ *authoritative;*: Supone que la configuración correcta para la red es la definida en el servidor DHCP y tratará de reasignar datos a los clientes mal configurados. Este parámetro puede ser global o asignando a una declaración de subred. Los cambios realizados en el servidor marcado como authoritative tienen una rápida propagación en la subred ya que se reconfigura cualquier cliente con la antigua configuración.
- ⇨ *subnet 192.168.0.0 netmask 255.255.255.0*: definimos la red en la que queremos hacer asignaciones y su máscara de subred.

- ⇨ *one-lease-per-client on;*: cuando esta opción está en "on" y un cliente solicita una asignación, el servidor libera automáticamente cualquier otra asignación que tenga ese cliente. Se supone que si el cliente hace una solicitud es porque ha olvidado que tuviera alguna, es decir tiene un solo interfaz de red. Si no se da esta situación en los clientes hay que usar este parámetro con precaución.
- ⇨ *option routers 192.168.0.254;*: definimos la puerta de enlace de la red.
- ⇨ *option netbios-name-servers 192.168.0.8;*: definimos la dirección del servidor WINS para NetBios, de nuevo coincide con la máquina local.
- ⇨ *range 192.168.0.11 192.168.0.51;*: definimos el rango de asignación de direcciones IP.

✎ **NOTA IMPORTANTE:** Es necesario otorgar permisos de escritura en la carpeta */etc/bind* al usuario con el cual se ejecuta el proceso bind para que la actualización dinámica se realice correctamente.

Instalación y configuración de *LAM(Ldap Account Manager)*

LAM es un frontend web para la administración de usuarios para cuentas unix y Samba dentro de un directorio LDAP.
Este paquete tiene dependencias, es necesario tener instalado tanto php4 o superior como apache, entre otros. Estas dependencias se supondrán satisfechas y correctamente configuradas.
Hay que destacar que la instalación de LAM es totalmente independiente respecto a la ubicación donde este instalado el OpenLDAP. Es decir, si se dispone de otra máquina donde ya este configurado el servidor Apache y php, podría ser instalado LAM en esa máquina y configurarlo, como se verá más adelante, para que apunte a la ubicación donde se encuentra el LDAP, aunque en este caso va a ser configurado en la misma máquina donde residen el resto de servicios de red(en el que se incluye LDAP).
En este caso no utilizaremos apt-get para su instalación, descargaremos la versión más reciente del paquete .deb(con soporte para idioma en castellano) de la página web(también necesario isntalar dos extensiones para php):

debian: # wget http://prdownloads.sourceforge.net/lam/ldap-account-manager_ 1.1.1- 1_ all.deb?download
debian: # apt-get install php-fpdf php4-mhash
debian: # dpkg -i ldap-account-manager_ 1.1.1-1_ all.deb

En la pantalla de configuración activaremos el soporte únicamente para apache(no para apache-ssl), a continuación estableceremos el *alias* de apache para la página web: en este caso hemos utilizado *lam*, pero podría ser seleccionado cualquier otro. Por último dejaremos el password establecido por

defecto *lam*, que más tarde modificaremos en el programa.
Para continuar la configuración, abriremos una ventana del navegador, e introduciremos: *http://debian/lam*. Seguidamente, seleccionaremos *LAM Configuration*(el password de acceso es *lam* (que configuramos previamente), después *Edit general settings* y modificaremos el pasword de acceso a la configuración, teclearemos *ads06*.

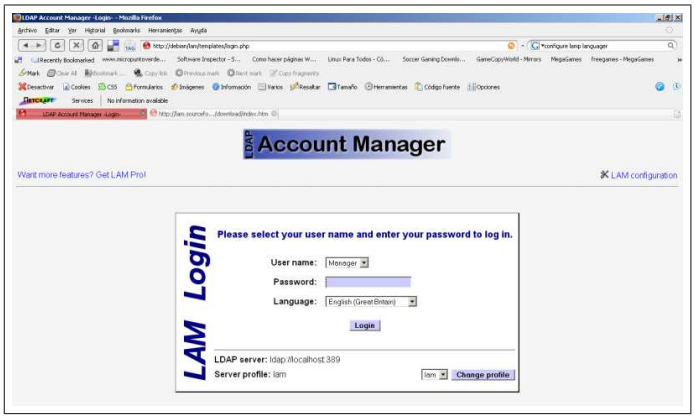

Figura 7: Pantalla de login de LAM

Figura 8: Pantalla LAM Configuration

Una vez modificado el password por defecto, configuraremos los parámetros del servidor ldap(mediante la opción *Edit server profiles*, el password de acceso es el mismo configurado previamente: *lam*

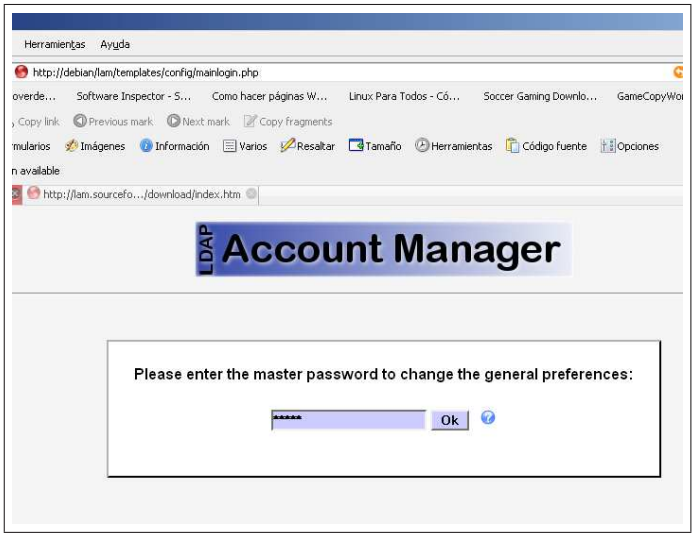

Figura 9: Pantalla de acceso de cambio de password

Figura 10: Pantalla de acceso de cambio de password

También es necesario configurar las unidades organizativas y DN's de LDAP mediante la opción *edit account types*:

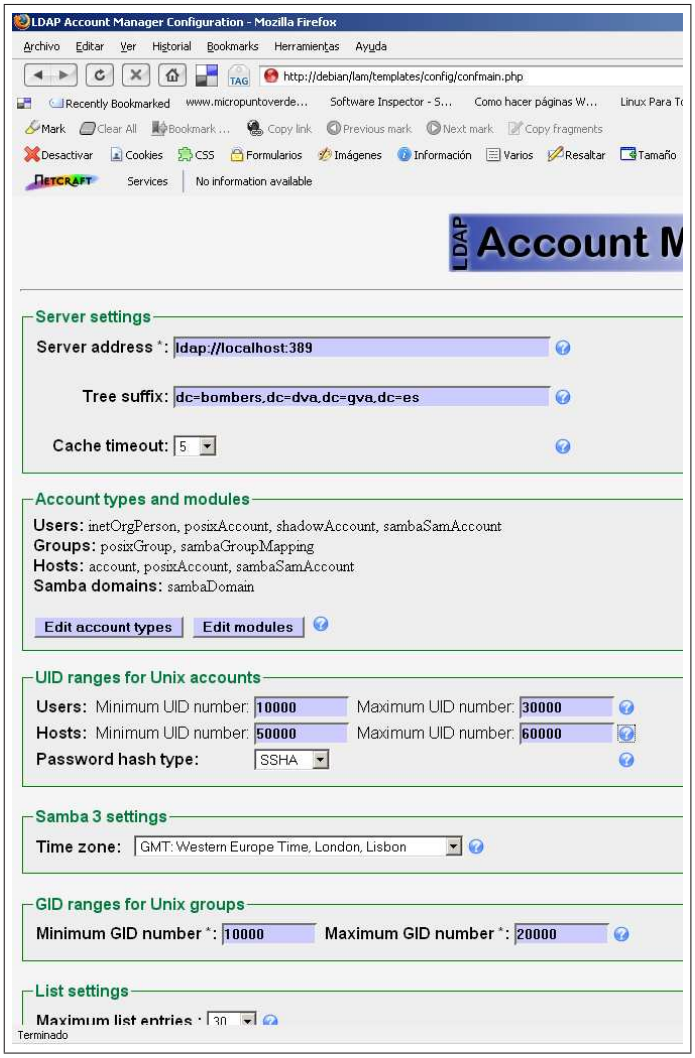

Figura 11: configuración de LDAP

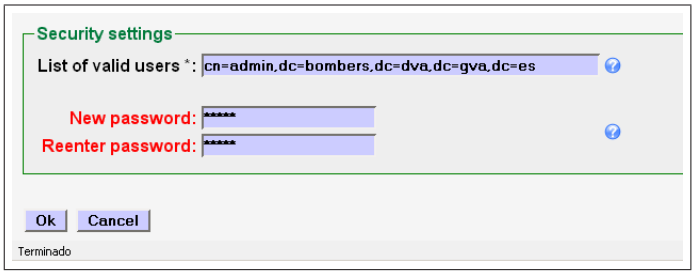

Figura 12: Configuración del usuario admin de LDAP

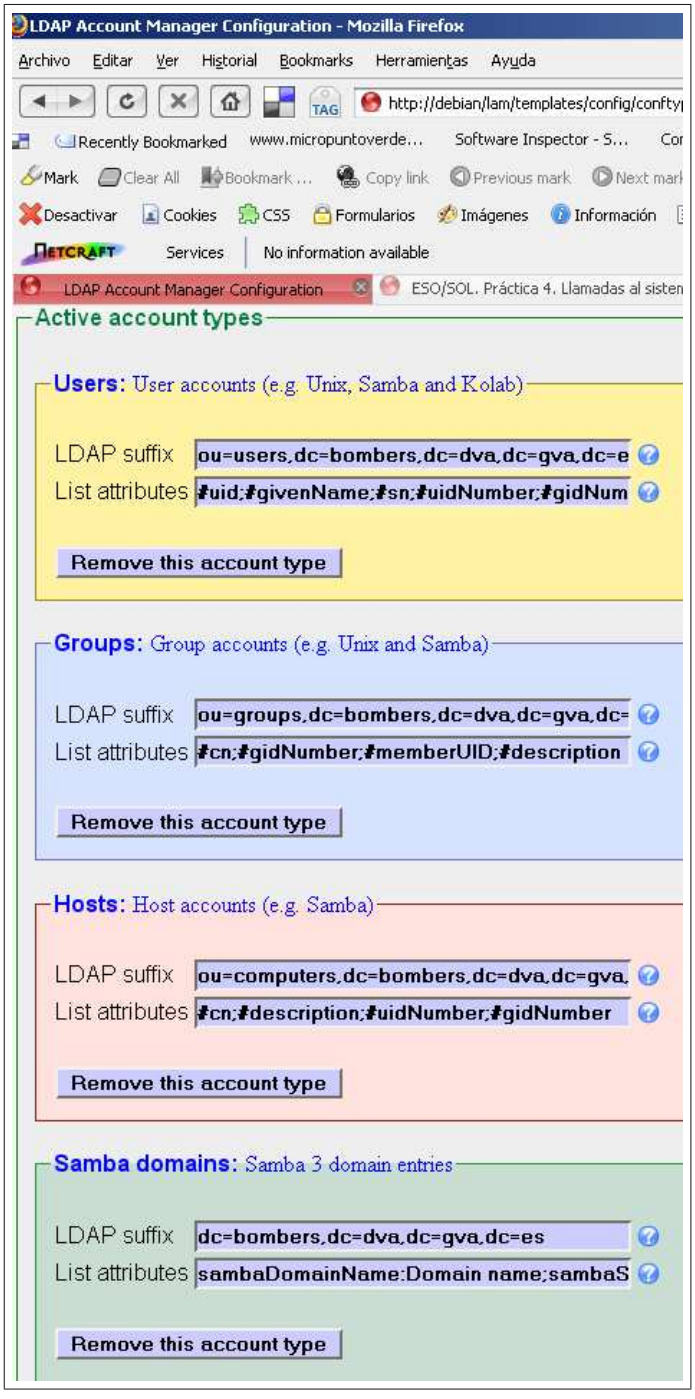

Figura 13: Configuración de las cuentas de LDAP

Una vez finalizada la configuración accederemos a la sección en la cual pueden gestionarse usuarios, grupos, equipos, dominio, etc...:

Figura 14: Sección de gestión de objetos LDAP

4.5. Migración a la infraestructura Linux.

Por motivos de privacidad y tratamiento de datos personales, los nombres de usuarios, carpetas compartidas y archivos, son de carácter meramente demostrativo, por lo que no coinciden en ningún caso con los datos electrónicos reales.
En primer lugar para realizar la exportación de las cuentas de usuarios utilizaremos las herramientas *Windows to Linux Migration Toolkit* que descargaremos de la web:
http://mesh.dl.sourceforge.net/sourceforge/w2lmt/w2lmt-0.3.1.tar.gz
Para migrar la información DNS editaremos el archivo *migrate-dns.conf*:

SourceHost="kame.bombers.dva.gva.es"
SourceDomain="bombers.dva.gva.es"
TargetConf="/tmp/named.conf"
TargetDbDir="/tmp"

Después ejecutaremos el script de migración el cual generará los dos archivos de zonas con la información necesaria:

debian:/opt/w2lmt-0.3.1# ./w2lmt-migrate-dns -f migrate-dns.conf

Generando dos archivos en la carpeta */tmp* que integraremos en el servidor DNS de Linux:

cp /tmp/ 0.168.192.rev /etc/bind/db.192.168.0
cp /tmp/bombers.dva.gva.es.hosts /etc/bind/db.bombers.dva.gva.es
*chmod g+w /etc/bind/**

A continuación descomprimiremos el archivo y editaremos el archivo de configuración *migrate-smbauth.conf*:

#source windows PDC host (typically DNS name)
SourceHost="kame.bombers.dva.gva.es"
#source windows domain name
SourceDomain="BOMBERS"
#source PDC type, can be NT4,AD
SourceType="NT4"
#source windows domain administrator account name
SourceAdminAccount="Administrador"
#target linux LDAP server
TargetHost="debian.bombers.dva.gva.es"
#target linux LDAP port (389 is default
TargetPort="389"
#location of config file for samba
smbconf="/etc/samba/smb.conf"
#location of config file for smbldap-toolkit
smbldap="/etc/smbldap-tools/smbldap.conf"

La información que es necesario indicar incluye el nombre la máquina que actúa como PDC en Windows 2000 Server y el nuevo PDC de Linux, también se indicará el usuario Administrador del dominio tanto del LDAP como el de Active Directory y la ruta de los archivos de configuración de Samba y sbmldap-tools.
Es necesario establecer el valor: **domain master = no** en el archivo de configuración de samba *smb.conf*, indicamos que el servidor Samba debe ser un controlador de dominio de reserva(BDC) para que esté autorizado para recibir una copia de los objetos de autenticación del dominio de Windows existente. Una vez concluida la migración y retirado el servidor Windows, modificaremos de nuevo el valor a **domain master = yes** y reiniciaremos Samba que pasará a ser de BDC a PDC.
A continuación ejecutaremos el script de migración(antes es necesario detener el servidor de SAMBA):

debian:/opt/w2lmt-0.3.1# ./w2lmt-migrate-smbauth -f migrate-smbauth-.conf
Enter password for Windows SAM Administrador:
Enter password for LDAP cn=admin,dc=bombers,dc=dva,dc=gva,dc=es:
Testing SAM connectivity to kame.bombers.dva.gva.es...ok
ready to migrate NT4 using the following parameters

LDAP Settings: ==========
Master LDAP Server: debian.bombers.dva.gva.es
Master LDAP Port: 389
Master DN: cn=admin,dc=bombers,dc=dva,dc=gva,dc=es
LDAP Base Suffix: dc=bombers,dc=dva,dc=gva,dc=es
Users OU: ou=Users,dc=bombers,dc=dva,dc=gva,dc=es
Groups OU: ou =Groups,dc=bombers,dc=dva,dc=gva,dc=es
Computers OU: ou=Computers,dc=bombers,dc=dva,dc=gva,dc=es
IDMap OU: ou=Idmap ,dc=bombers,dc=dva,dc=gva,dc=es
Unix ID Pool DN: sambaDomainName=BOMBERS,dc=bombers,dc=-dva,dc=gva,dc=es

SAMBA Settings: ==========
User's Home Share: \\DEBIAN\ %U
User's Login Script:
User's Profile: \\DEBIAN\profiles\ %U
Password Age: 45
User Default GID: 513
Computer Default GID: 515

POSIX Settings: ==========
User's Home Directory: /home/ %U
Default Shell: /bin/bash
Default Mail Domain:
Skeleton Directory: /etc/skel
Hash Encryption Type: SSHA
Hash Encryption Salt:

El script lleva a cabo las siguientes acciones:

- Solicita las contraseñas de los servidores origen(Windows) y de destino(Openldap).
- Enumera el SID del dominio y se une al dominio NT como un BDC.
- Crear las OU necesarias en OpenLDAP y enumera los objetos de grupo.
- Procesa información de miembros de grupos y modifica los objetos de grupo a fin de agregar información de pertenencia uid.

El siguiente paso consistiría en consultar al servidor de Active Directory a fin de actualizar los objetos anteriores con información no relacionada con

		Group name	GID number	Group members	Group description
	Filter				
	Edit	Acceso compatible con Pre-Windows 2000	1020		Un grupo de compatibilidad anterior que permite acceso de lectura todos los usuarios y grupos en el dominio
	Edit	Account Operators	548		Pueden administrar cuentas de usuarios y grupos de dominio
	Edit	Administradores de esquema	1003	Administrador	Administradores designados del esquema
	Edit	Administradores DHCP	1015		Miembros que tienen acceso administrativo al servicio DHCP
	Edit	Administrators	544		Los administradores tienen acceso completo y sin restricciones al equipo o dominio
	Edit	Admins. del dominio	1000	Administrador	Administradores designados del dominio
	Edit	Backup Operators	551		Los operadores de copia pueden sobrescribir restricciones de seguridad con el único propósito de hacer copias de seguridad o restaurar archivos
	Edit	comercial	1007	antonio	
	Edit	contabilidad	1008	paloma	
	Edit	Controladores de dominio	1001	KAME$; debian$	Todos los controladores de dominio del dominio
	Edit	desarrollo	1009	elena	
	Edit	DnsAdmins	1016		Grupo de administradores de DNS
	Edit	DnsUpdateProxy	1006		Clientes DNS que tienen permiso para efectuar actualizaciones dinámicas en nombre de otros clientes (tales como servidores DH
	Edit	Domain Admins	512	Administrador	Netbios Domain Administrators
	Edit	Domain Computers	515		Todas los servidores y estaciones de trabajo unidos al dominio
	Edit	Domain Guests	514		Todos los invitados del dominio
	Edit	Domain Users	513	Invitado; TsInternetUser; antonio; eduardo; elena; fernando; krbtgt; nobody; paloma	Todos los usuarios del dominio
	Edit	gerencia	1010	fernando	

Figura 15: Grupos creados en LDAP tras script de migración

el proceso de autenticación, como la dirección de correo electrónico, número de teléfono, pero en este caso dicha información no es relevante para el cliente y por tanto va a ser obviada y no se realizará la migración.

Finalmente realizaremos la migración de los permisos de archivos de Windows a Linux:
para ver los recursos compartidos que tiene la máquina con Windows 2000 Server ejecutaremos en el servidor linux:

debian: # net rpc share -S kame -Uadministrador
Password:
contabilidad
comercial
informatica
gerencia
IPC$
NETLOGON
desarrollo
homes
ADMIN$
SYSVOL

C$
A continuación crearemos físicamente dichos recursos en linux y los compartiremos con Samba:

debian:/# mkdir /mnt/contabilidad
debian:/# mkdir /mnt/comercial
debian:/# mkdir /mnt/informatica
debian:/# mkdir /mnt/gerencia
debian:/# mkdir /mnt/desarrollo
debian:/# mkdir /mnt/NETLOGON

[NETLOGON]
comment = Network Logon Service
path = /mnt/NETLOGON
guest ok = Yes
locking = no
browseable = no

[contabilidad]
path = /mnt/contabilidad
read only = No
profile acls = Yes

[comercial]
path = /mnt/comercial
read only = No
profile acls = Yes

[informatica]
path = /mnt/informatica
read only = No
profile acls = Yes

[gerencia]
path = /mnt/gerencia
read only = No
profile acls = Yes

[desarrollo]
path = /mnt/desarrollo
read only = No

profile acls = Yes

[profiles]
path = /home/profiles
force user = %U
read only = No
create mask = 0600
directory mask = 0700
guest ok = Yes
profile acls = Yes
browseable = No
csc policy = disable

Una vez creados los recursos compartidos, realizaremos la exportación de permisos de las carpetas compartidas de windows mediante la utilidad *xcalcs.exe* en el PDC de Windows:

xcacls gerencia /T > gerencia.txt
xcacls contabilidad /T > contabilidad.txt
xcacls desarrollo /T > desarrollo.txt
xcacls informatica /T > informatica.txt
xcacls comercial /T > comercial.txt

Si mostramos el archivo donde se han volcado los archivos, por ejemplo del recurso contabilidad:

C:\comercial BUILTIN\Administradores:(OI)(CI)F
BOMBERS\comercial:(OI)(CI)F
BOMBERS\gerencia:(OI)(CI)R

Las letras entre paréntesis indican: *OI*: se establecerá la herencia de permisos en todos los archivos de este directorio, *CI*: se establecerá la herencia de permisos en todas las carpetas de este directorio. La letra *F* significa control total de acceso y la *R*, únicamente permisos de lectura.
A continuación estableceremos las ACL's necesarias en los recursos compartidos de Linux:

Por ejemplo, si visualizamos las acl´s de la carpeta contabilidad:
C:\contabilidad BUILTIN\Administradores:(OI)(CI)F
BOMBERS\contabilidad:(OI)(CI)F
BOMBERS\gerencia:(OI)(CI)R

Estableceremos las siguientes acl's con el comando *setfacl* y eliminamos el

acceso al grupo seguridad otros de unix(se utiliza la opción -d "ACL predeterminada", para que los nuevos archivos y directorios creados en la carpeta heredarán las acl's):

debian:/mnt#setfacl -d -m group:Domain Admins:rwx,group:comercial:rwx, group:gerencia:r comercial
debian:/mnt# chmod -R o-rwx comercial debian:/mnt# chgrp comercial comercial

Si obtenemos las propiedades de las acl's del archivo:

debian:/mnt# getfacl comercial
 # file: comercial
 # owner: root
 # group: root
user::rwx
user:root:rwx
group::r-x
group:Domain Admins:rwx
group:comercial:rwx
group:gerencia:r–
mask::rwx
other::—

Realizaremos los mismos pasos para el resto de carpetas consultado para ellos los archivos txt con las acl's extraídas de windows:

debian:/mnt# chmod -R o-rwx contabilidad
debian:/mnt# chgrp contabilidad contabilidad
debian:/mnt# chmod -R o-rwx desarrollo
debian:/mnt# chgrp desarrollo desarrollo
debian:/mnt# chmod -R o-rwx gerencia
debian:/mnt# chgrp gerencia gerencia
debian:/mnt# chmod -R o-rwx informatica
debian:/mnt# chgrp informatica informatica
debian:/mnt# chmod -R o-rwx NETLOGON
debian:/mnt#setfacl -R -d -m group:Domain Admins:rwx,group:contabilidad:rwx,group:gerencia:r contabilidad
debian:/mnt#setfacl -R -d -m group:Domain Admins:rwx,group:desarrollo:-rwx,group:gerencia:r desarrollo
debian:/mnt#setfacl -R -d -m group:Domain Admins:r,group:gerencia:rwx gerencia
debian:/mnt#setfacl -R -d -m group:gerencia:r,group:informatica:rwx infor-

matica
debian:/mnt#setfacl -R -d -m group:Domain Users:rwx NETLOGON

Para que los recursos compartidos de Samba puedan aceptar las nuevas ACL POSIX es necesario añadir la siguiente línea al archivo de configuración smb.conf y recargar la configuración de samba:

map acl inherit = Yes
debian:/mnt# /etc/init.d/samba reload

También es necesario tener en cuenta la carpeta *profiles* situada en la ruta *\home\profiles* que almacena la configuración del escritorio y de los accesos a las aplicaciones de los usuarios por lo que es necesario otorgar permisos de acceso a todos los usuarios del dominio:
debian:/home# chgrp -R Domain Users profiles
debian:/mnt# setfacl -R -d -m group:Domain Admins:rwx,group: Domain Users:rwx profiles

4.6. Prueba de la infraestructura Linux.

Como prueba del correcto funcionamiento del nuevo Controlador de Dominio, realizaremos la integración de un cliente con *Windows XP*:

El único paso a realizar antes de unir el equipo al dominio es modificar una clave del registro de windows mediante el comando *regedit*:
Ejecutaremos regedit y modificaremos el valor de "1" a "0" en la clave: **HKEY_LOCAL_MACHINE_SYSTEM\CurrentControlSet\Services \Netlogon\Parameters\RequireSignOrSeal**

A continuación procederemos a unir el equipo al dominio:

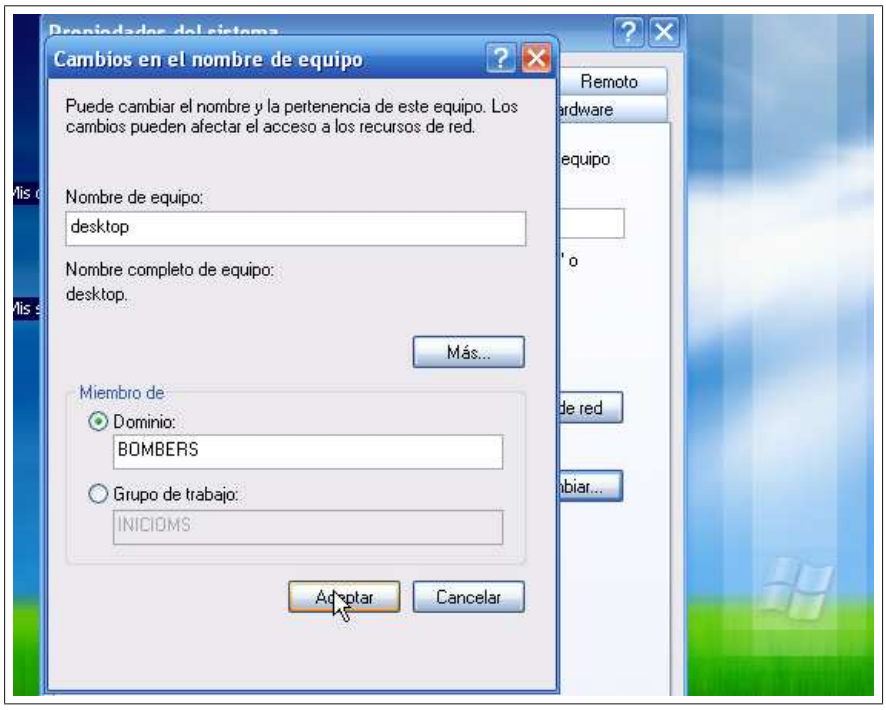

Figura 16: Unir equipo al dominio, paso 1

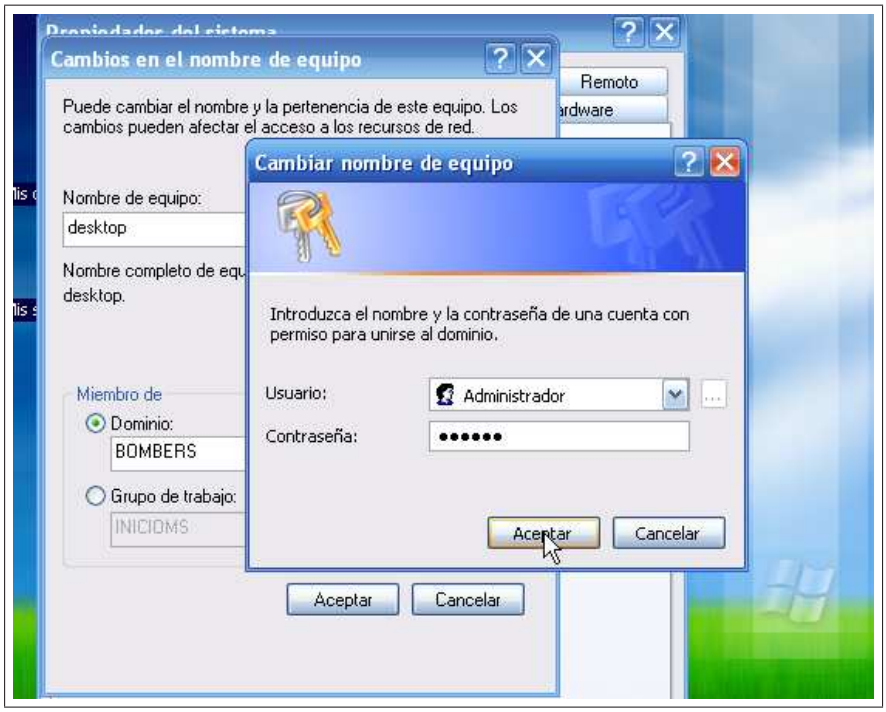

Figura 17: Unir equipo al dominio, paso 2

Figura 18: Unir equipo al dominio, paso 3

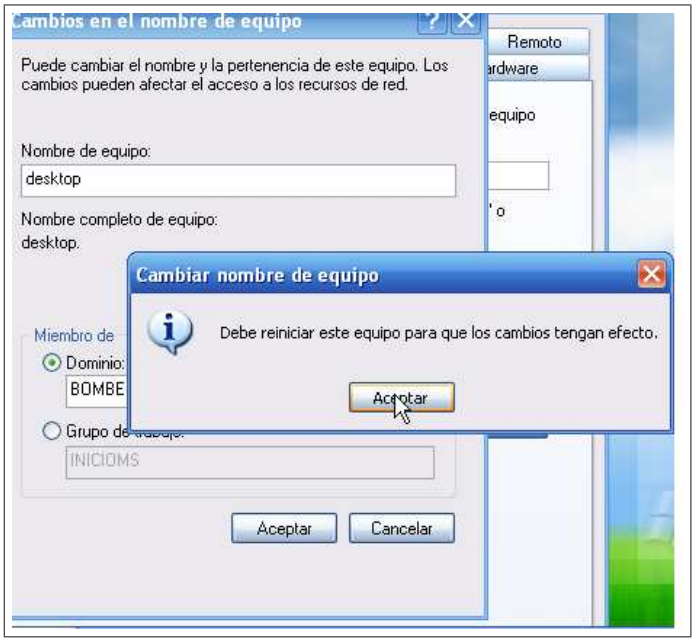

Figura 19: Unir equipo al dominio, paso 4

✎ **NOTA IMPORTANTE:** Si al intentar unir el equipo al dominio con el usuario *Administrador* obtenemos un error *carece de permisos para unirse al dominio* será necesario otorgar al usuario Administrador privilegios para permitir añadir cuentas de equipos al dominio:

debian: # net -U Administrador rpc rights list
SeMachineAccountPrivilege Add machines to domain
SePrintOperatorPrivilege Manage printers
SeAddUsersPrivilege Add users and groups to the domain
SeRemoteShutdownPrivilege Force shutdown from a remote system
SeDiskOperatorPrivilege Manage disk shares

debian: # net -U Administrador rpc rights grant Administrador SeMachineAccountPrivilege
Password:
Successfully granted rights.

Una vez se ha unido al dominio el equipo es necesario otorgar permisos de acceso a los usuarios del dominio a la clave del registro con la aplicación *regedit*:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

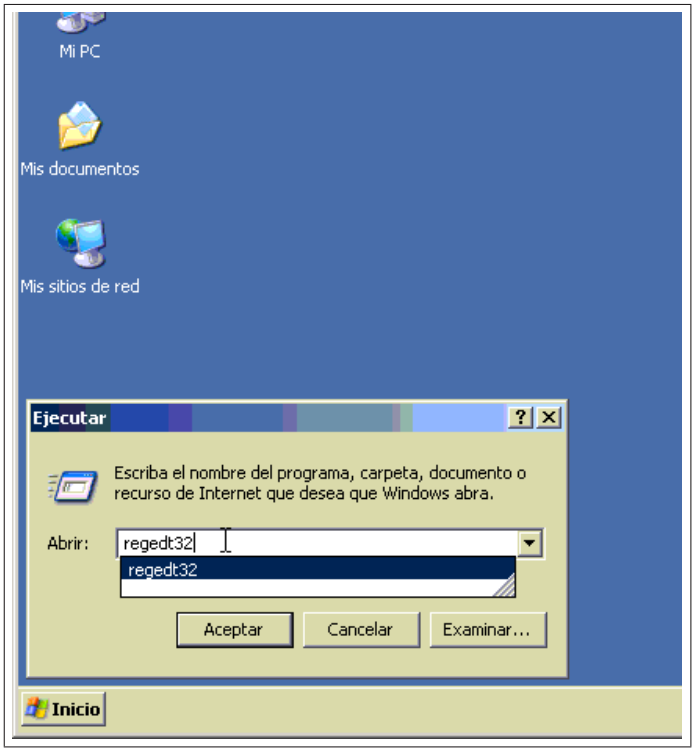

Figura 20: Modificar registro, paso 1

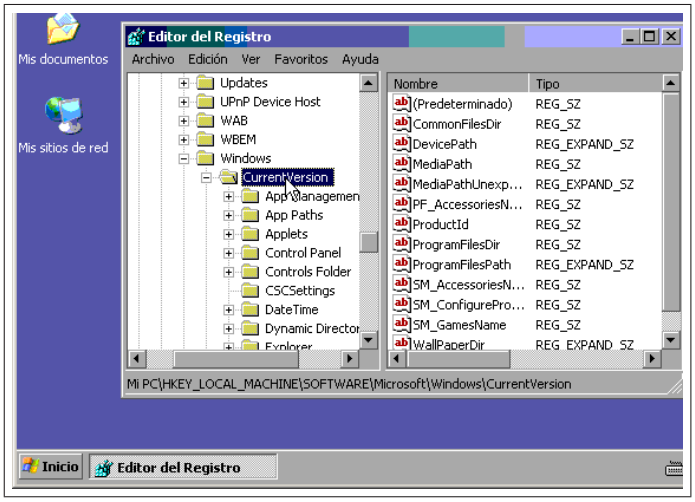

Figura 21: Modificar registro, paso 2

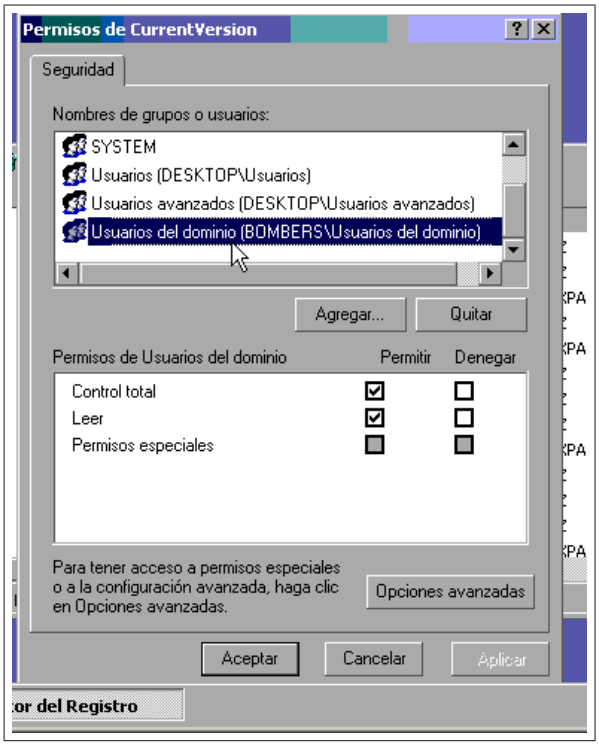

Figura 22: Modificar registro, paso 3

4.6.1. Creación de un plan de pruebas.

Como último paso antes de pasar a producción el nuevo servidor se realizará

un plan de pruebas en el cliente Windows para verificar que se cumplen todos los requisitos exigidos de cada uno de los servicios migrados:

Asignación de direcciones IP

El servidor DHCP otorga correctamente la IP del rango establecido asignando correctamente también la puerta del enlace y el servidor DNS:

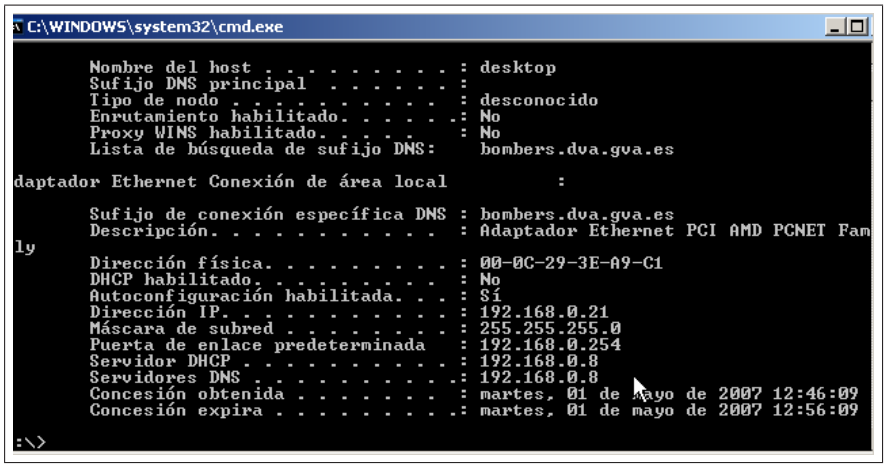

Figura 23: Asignación de dirección IP

Resolución de nombres dinámica

Cuando se agrega cualquier equipo al dominio, se añade dinámicamente al archivo de zonas del servidor DNS independientemente de la IP asignada por el servidor DHCP:

debian: # host -l bombers.dva.gva.es
bombers.dva.gva.es name server debian.bombers.dva.gva.es.
gc._msdcs.bombers.dva.gva.es has address 192.168.0.8
debian.bombers.dva.gva.es has address 192.168.0.8
desktop.bombers.dva.gva.es has address 192.168.0.21

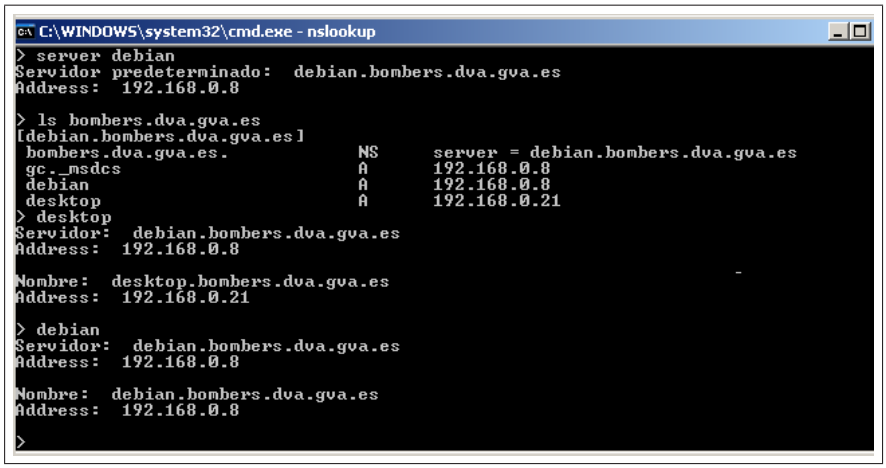

Figura 24: Resolución de nombres

Administración de permisos(Control de Acceso)

Accediendo por red a las carpetas compartidas en el nuevo servidor podemos comprobar la restricción de accesos y permisos configurados previamente(accedemos al sistema con el usuario *eduardo*:

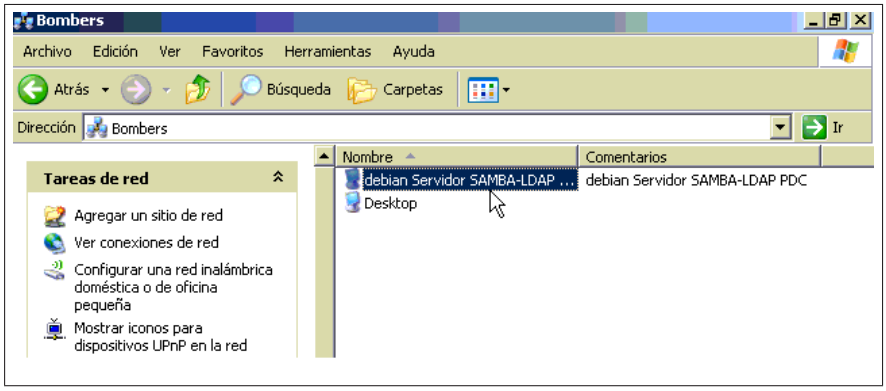

Figura 25: Acceso a carpetas compartidas

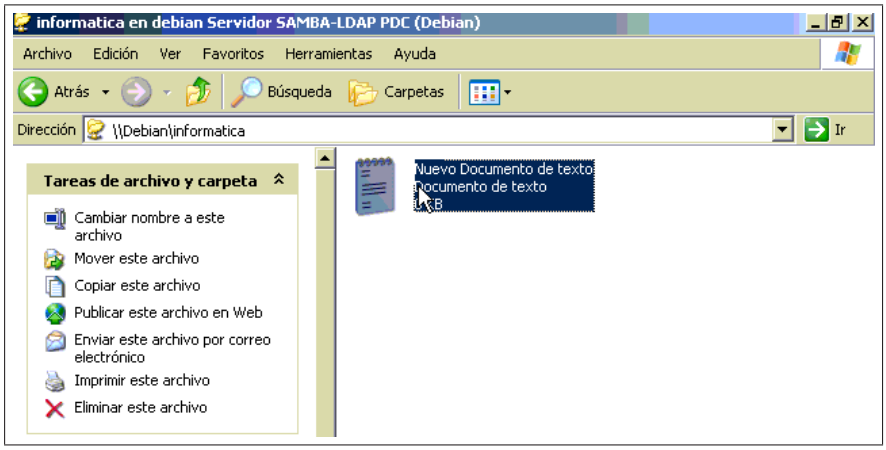

Figura 26: Creación de un documento de texto

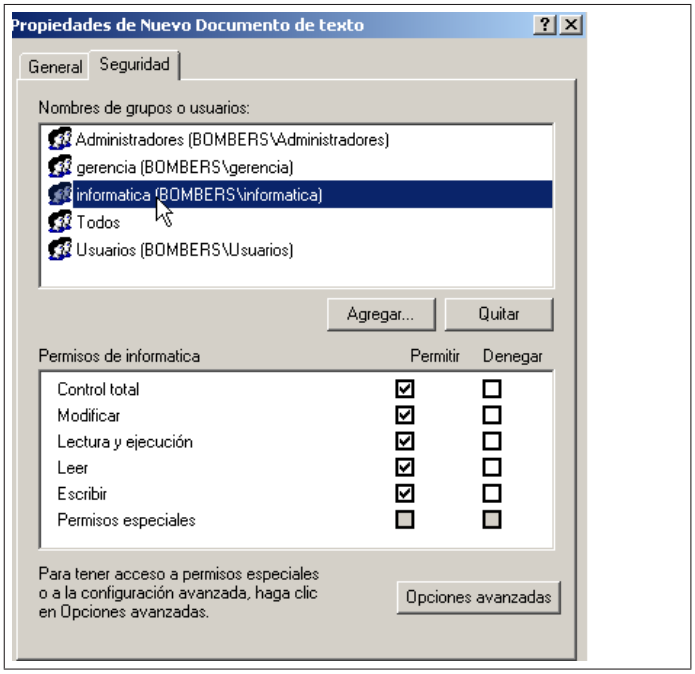

Figura 27: Permisos aplicados a nuevos documentos creados

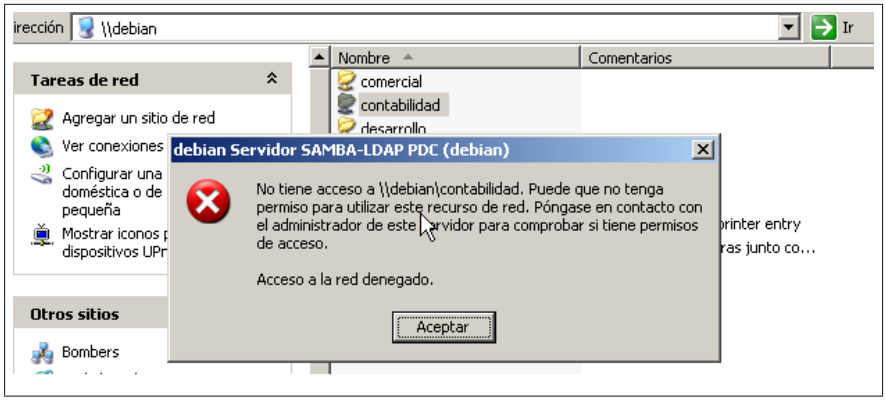

Figura 28: Los permisos asignados a las carpetas se aplican correctamente

5. Bibliografía

Referencias

[All05] D. y colbs. Allen. *Herramientas de migración de Windows a Linux*. Anaya Multimedia, 2005.

[aut] Varios autores. http://www.dwheeler.com/oss_fs_why.html. Technical report.

[aut04] Varios autores. *Linux Client Migration Cookbook- A practical guide Planning and Implementation Guide for Migrating to Desktop Linux.* ibm.com/Redbooks, 2004.

[aut05] Varios autores. *Migration guide.* Berlin. Federal Ministry of the Interior, 2005.

[miga] http://www.debianhelp.co.uk/acl.htm. Technical report.

[migb] http://www.debian.org. Technical report.

[migc] http://www.novell.com. Technical report.

[migd] http://www.redhat.com. Technical report.

6. Lista de Figuras

Índice de figuras

7. Lista de Tablas

Índice de cuadros